CHAPTER 2

AnyConnect Secure Mobility Client の展開

ASA からか、エンタープライズ ソフトウェア管理システム（SMS）を使用して、リモート ユーザに Cisco AnyConnect Secure Mobility Client を展開できます。

ASA から展開された場合、リモート ユーザは、ASA への最初の SSL 接続を行います。リモート ユーザは、クライアントレス SSL VPN 接続を受け入れるように設定されている ASA の IP アドレスまたは DNS 名をブラウザに入力します。ブラウザ ウィンドウにログイン画面が表示され、ユーザがログインおよび認証に成功すると、コンピュータのオペレーティング システムに対応したクライアントがダウンロードされます。ダウンロード後、クライアントは自動的にインストールおよび設定され、ASA への IPsec（IKEv2）接続または SSL 接続が確立されます。

Cisco AnyConnect Secure Mobility Client バージョン 3.0 では、新規モジュールが AnyConnect クライアント パッケージと統合されています。ASA を使用して AnyConnect を展開する場合、ASA では、すべてのオプション モジュールも展開できます。ASA によって AnyConnect クライアントおよびさまざまなモジュールを展開する方法を「Web 展開」と呼びます。

SMS を使用して AnyConnect ソフトウェアをエンドポイントに配布し、エンドポイントが ASA に接続する前にインストールする方法を「事前展開」と呼びます。この方法を使用すると、VPN サービスを実現するコア クライアントおよびオプション モジュールを展開できますが、インストール順序およびその他の詳細事項に特に注意する必要があります。

バージョン 3.0 には、ASA への SSL と IPsec（IKEv2）によるセキュア VPN 接続を実現するコア AnyConnect VPN クライアントの他に、次のモジュールがあります。

- ネットワーク アクセス マネージャ
- ポスチャ評価
- テレメトリ
- Web セキュリティ
- AnyConnect Diagnostic and Reporting Tool（DART）
- Start Before Logon（SBL）

ここでは、次の項目について説明します。

- 「スタンドアロン AnyConnect プロファイル エディタの使用」（P.2-44）
- 「AnyConnect Secure Mobility ソリューションの WSA をサポートするための ASA の設定」（P.2-49）

（注）　ASA にデフォルトの内部フラッシュ メモリ サイズまたはデフォルトの DRAM サイズ（キャッシュ メモリ用）だけがある場合、ASA 上で複数の AnyConnect クライアント パッケージを保存およびロードすると、問題が発生することがあります。この制限事項は、オプション モジュールを含む AnyConnect 3.0 クライアントの場合、特に該当します。フラッシュ メモリにパッケージ ファイルを保持するために十分な容量がある場合でも、クライアント イメージの unzip とロードのときに ASA のキャッシュ メモリが不足する場合があります。AnyConnect を使用する場合の ASA のメモリ要件について、および ASA で行えるメモリ アップグレードについて詳しくは、Cisco ASA 5500 シリーズの最新のリリース ノートを参照してください。

AnyConnect クライアント プロファイルの概要

Cisco AnyConnect Secure Mobility Client 機能は、AnyConnect プロファイルでイネーブルにします。プロファイルは、コア クライアントと VPN 機能のための設定およびオプション クライアント モジュール（ネットワーク アクセス マネージャ、ポスチャ、テレメトリ、Web セキュリティ）のための設定を含む XML ファイルであり、複数ファイルあります。ASA は AnyConnect のインストールおよび更新中にプロファイルを展開します。ユーザがプロファイルの管理や修正を行うことはできません。

プロファイルは、ASDM から起動する、GUI ベースの便利なツールである、AnyConnect プロファイル エディタを使用して設定できます。Windows 用 AnyConnect ソフトウェア パッケージ バージョン 2.5 以降には、エディタが含まれています。このエディタは、AnyConnect パッケージを ASA にロードし、AnyConnect クライアント イメージとして指定するとアクティブ化されます。

ASDM に統合されたプロファイル エディタの代わりに、Windows 用プロファイル エディタのスタンドアロン バージョンも使用できます。クライアントを事前展開する場合は、ソフトウェア管理システムを使用してコンピュータに展開する、VPN サービス用のプロファイルおよびその他のモジュールを、スタンドアロンのプロファイル エディタを使用して作成できます。

これで、クライアント プロファイル XML ファイルを手動で編集し、プロファイルとして ASA にインポートできます。

2 つのバージョンの Cisco AnyConnect プロファイル エディタは、テレメトリ クライアント プロファイルを設定するプロファイル エディタには「スタンドアロン」バージョンがない点が異なり、各エディタは別々に配布、起動されます。その他のすべての点は、2 つのバージョンのプロファイル エディタで同一です。

ASA は、すべての AnyConnect ユーザにグローバルにプロファイルを展開するか、ユーザのグループ ポリシーに基づいて展開するように設定できます。通常、ユーザは、インストールされている AnyConnect モジュールごとに 1 つのプロファイル ファイルを持ちます。1 人のユーザに複数の VPN プロファイルを割り当てる必要があることがあります。複数の場所で作業するユーザは、複数の VPN プロファイルを必要とすることがあります。Start Before Logon など、一部のプロファイル設定は、グローバル レベルで接続を制御します。その他の設定は、特定のホストに固有であり、選択したホストによって異なります。

（注）　プロファイルが複数ある場合、AnyConnect では、プロファイル内のサーバ リストを統合して、GUI のドロップリストにすべてのサーバを表示します。ユーザがサーバを選択すると、そのサーバを含むプロファイルが AnyConnect で使用されます。一方、接続後は、その ASA 上に設定されているプロファイルが使用されます。

一部のプロファイル設定は、ユーザ コンピュータ上のユーザ プリファレンス ファイルまたはグローバル プリファレンス ファイルにローカルに保存されます。ユーザ ファイルには、AnyConnect クライアントが、クライアント GUI の [プリファレンス（Preferences）] タブにユーザ制御可能設定を表示するうえで必要となる情報、およびユーザ、グループ、ホストなど、直近の接続に関する情報が保存されます。

グローバル ファイルには、ユーザ制御可能設定に関する情報が保存されます。これにより、ログイン前でも（ユーザがいなくても）それらの設定を適用できます。たとえば、クライアントでは Start Before Logon や起動時自動接続が有効になっているかどうかをログイン前に認識する必要があります。各オペレーティング システムで使用されるファイル名およびパスについては、「すべてのオペレーティング システムに対するプロファイルの場所」の表 2-15 を参照してください。クライアント プロファイルの作成の詳細については、次の各項を参照してください。

- 「統合された AnyConnect プロファイル エディタを使用した AnyConnect クライアント プロファイルの作成と編集」（P.2-3）
- 「スタンドアロン AnyConnect プロファイル エディタの使用」（P.2-44）

統合された AnyConnect プロファイル エディタを使用した AnyConnect クライアント プロファイルの作成と編集

ここでは、ASDM からプロファイル エディタを起動する方法、およびプロファイルを新規作成する方法について説明します。

Cisco AnyConnect Secure Mobility Client ソフトウェア パッケージ バージョン 2.5 以降（すべてのオペレーティング システム用）にはプロファイル エディタが含まれています。プロファイル エディタは、ASA 上で AnyConnect ソフトウェア パッケージを SSL VPN クライアント イメージとしてロードした時点で ASDM によりアクティブ化されます。

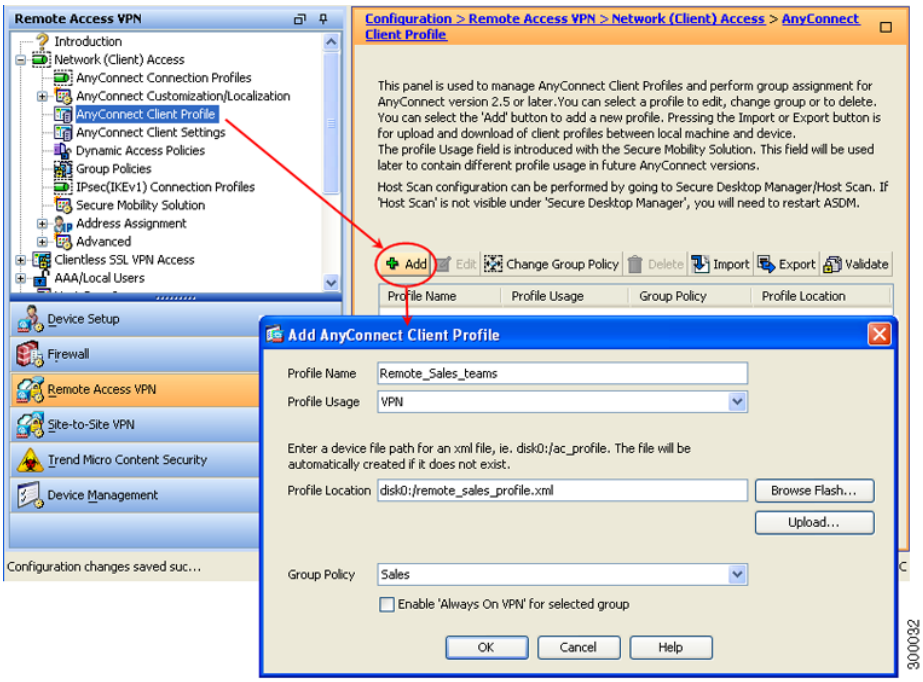
複数の AnyConnect パッケージをロードした場合は、最新の AnyConnect パッケージからプロファイル エディタがロードされます。これによりエディタには、旧バージョンのクライアントで使用される機能に加え、ロードされた最新の AnyConnect で使用される機能が表示されます。

ASDM でプロファイル エディタをアクティブ化する手順は次のとおりです。

ステップ 1　AnyConnect ソフトウェア パッケージを SSL VPN イメージとしてロードします。まだ行っていない場合は、第 2 章「AnyConnect をダウンロードするための ASA の設定」を参照してください。

ステップ 2　[設定（Configuration）] > [リモート アクセス VPN（Remote Access VPN）] > [ネットワーク（クライアント）アクセス（Network (Client) Access）] > [AnyConnect クライアント プロファイル（AnyConnect Client Profile）] を選択します。[AnyConnect クライアント プロファイル（AnyConnect Client Profile）] ペインが開きます。[追加（Add）] をクリックします。[AnyConnect クライアント プロファイルの追加（Add AnyConnect Client Profile）] ウィンドウが開きます（図 2-1）。

図 2-1　AnyConnect プロファイルの追加



ステップ 3　プロファイル名を指定します プロファイルの場所として別の値を指定していない場合、ASDM では、ASA フラッシュ メモリ上に同じ名前でクライアント プロファイル ファイルを作成します。

ステップ 4　[プロファイルの使用（Profile Usage）] フィールドで、作成するクライアント プロファイルのタイプを、VPN、ネットワーク アクセス マネージャ、Web セキュリティ、またはテレメトリから指定します。

ステップ 5　グループ ポリシーを選択します（任意）。ASA は、このプロファイルをグループ ポリシー内の全 AnyConnect ユーザに適用します。

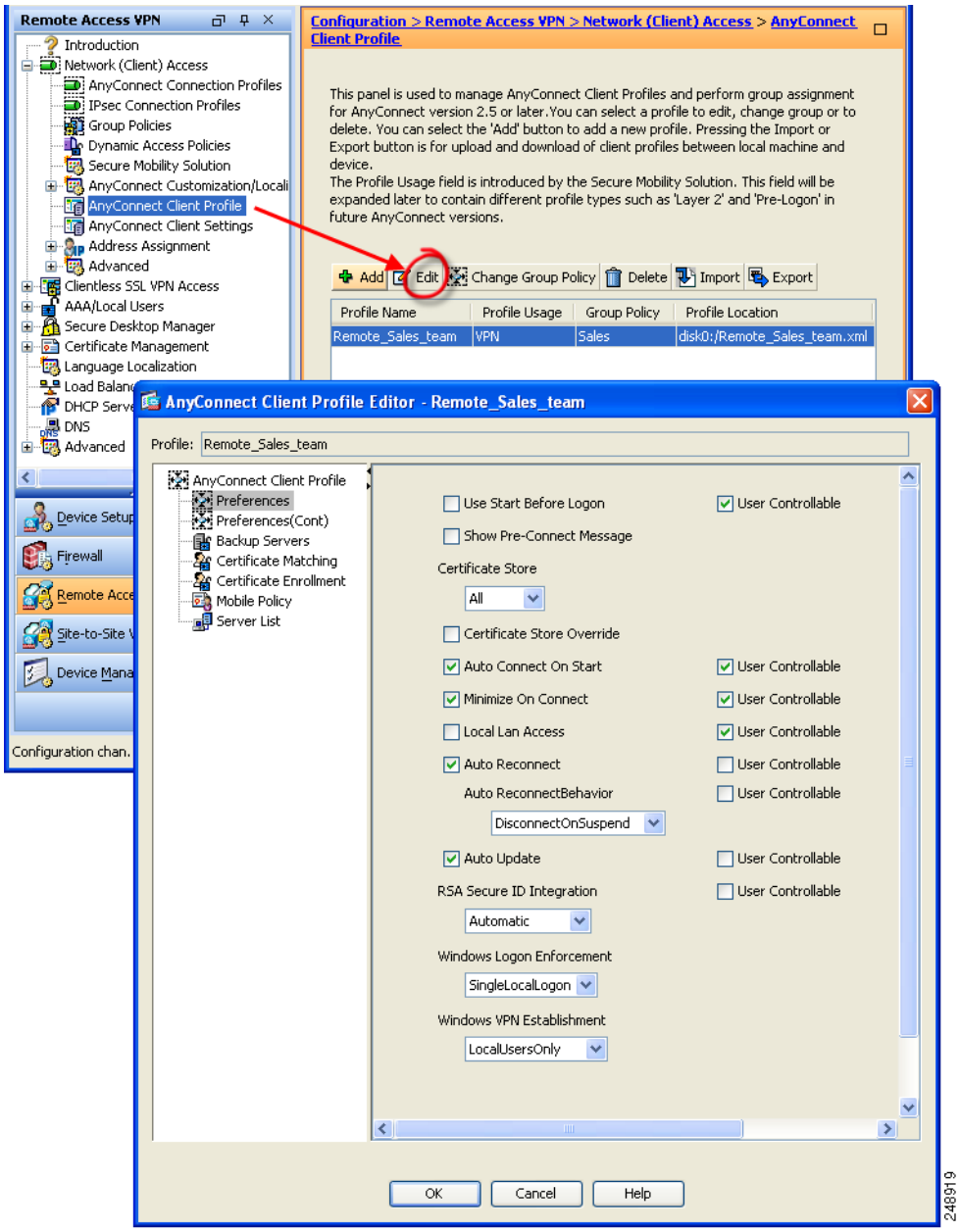
ステップ 6　[OK] をクリックします。ASDM によりプロファイルが作成され、そのプロファイルはプロファイル テーブルに表示されます。

ステップ 7　作成されたばかりのプロファイルをプロファイル テーブルから選択します。[編集（Edit）] をクリックします。プロファイル エディタが表示されます（図 2-2）。プロファイル エディタの各ペインで、AnyConnect 機能を有効にします。終了したら、[OK] をクリックします。

ステップ 8　[適用（Apply）] をクリックします。

ステップ 9　ASDM を終了して再起動します。

図 2-2　VPN クライアント プロファイルの編集例



AnyConnect クライアント プロファイルの展開

AnyConnect クライアント プロファイルは、以下の方法を使用して展開できます。

- 「ASA からの AnyConnect クライアント プロファイルの展開」（P.2-6）
- 「スタンドアロン プロファイル エディタで作成したクライアント プロファイルの展開」（P.2-7）

ASA からの AnyConnect クライアント プロファイルの展開

AnyConnect にプロファイルを展開するには、次の手順に従って ASA を設定します。

ステップ 1　「統合された AnyConnect プロファイル エディタを使用した AnyConnect クライアント プロファイルの作成と編集」（P.2-3）に従って、クライアント プロファイルを作成します。

ステップ 2　ASDM に統合されているプロファイル エディタを使用して、インストールするモジュール用のクライアント プロファイルを作成します。さまざまなクライアント プロファイルの設定手順については、次の章を参照してください。

- 第 3 章「VPN アクセスの設定」

（注）　最初の接続に関するユーザ制御可能なすべての設定をクライアント GUI に表示するには、VPN プロファイル サーバ リストに ASA を含める必要があります。それ以外の場合、フィルタは適用されません。たとえば、証明書照合を作成し、証明書が基準と適切に一致した場合でも、ASA がそのプロファイルにホスト エントリとして存在しない場合、この証明書照合は無視されます。詳細については、「サーバ リストの設定」（P.3-54）を参照してください。

- 第 4 章「ネットワーク アクセス マネージャの設定」
- 第 6 章「Web セキュリティの設定」
- 第 7 章「WSA に対する AnyConnect テレメトリの設定」

ステップ 3　クライアント プロファイルをグループ ポリシーと関連付けます。ASDM で、[設定（Configuration）] > [リモート アクセス VPN（Remote Access VPN）] > [ネットワーク（クライアント）アクセス（Network (Client) Access）] > [AnyConnect クライアント プロファイル（AnyConnect Client Profile）] を選択します。

ステップ 4　グループと関連付けるクライアント プロファイルを選択し、[グループ ポリシーの変更（Change Group Policy）] をクリックします。

ステップ 5　[プロファイルのグループ ポリシー＜ポリシー名＞の変更（Change Group Policy for Profile ***policy name***）] ウィンドウで、[使用可能なグループ ポリシー（Available Group Policies）] フィールドからグループ ポリシーを選択し、右矢印をクリックして [選択されたグループ ポリシー（Selected Group Policies）] フィールドに移動します。

ステップ 6　[OK] をクリックします。

ステップ 7　[AnyConnect クライアント プロファイル（AnyConnect Client Profile）] ページで、[適用（Apply）] をクリックします。

ステップ 8　[保存（Save）] をクリックします。

ステップ 9　設定が終了したら、[OK] をクリックします。

スタンドアロン プロファイル エディタで作成したクライアント プロファイルの展開

スタンドアロン プロファイル エディタを使用して作成したクライアント プロファイルの展開手順については、「事前展開された AnyConnect モジュールのインストール」（P.2-32）を参照してください。スタンドアロン AnyConnect プロファイル エディタのインストールと使用の手順については、「スタンドアロン AnyConnect プロファイル エディタの使用」（P.2-44）を参照してください。

AnyConnect を Web 展開する ASA の設定

この項では、次のトピックについて取り上げます。

- 「ASA 展開用の AnyConnect ファイル パッケージ」（P.2-7）
- 「AnyConnect の正常インストールの確認」（P.2-7）
- 「AnyConnect をダウンロードするための ASA の設定」（P.2-18）
- 「追加機能で使用するモジュールのイネーブル化」（P.2-23）

ASA 展開用の AnyConnect ファイル パッケージ

表 2-1 に、ASA による AnyConnect 展開用の AnyConnect ファイル パッケージの名前を示します。

表 2-1　ASA 展開用の AnyConnect パッケージ ファイル名

OS	ASA にロードされる AnyConnect 3.0 Web 展開パッケージ名
Windows	anyconnect-win-(ver)-k9.pkg
Mac	anyconnect-macosx-i386-(ver)-k9.pkg
Linux	anyconnect-linux-(ver)-k9.pkg

AnyConnect の正常インストールの確認

AnyConnect Secure Mobility Client がユーザ コンピュータに正常にインストールされたことを確認するには、次の項を確認してください。

- 「証明書に関するユーザ プロンプトを最小限にする」（P.2-8）
- 「AnyConnect 用 Cisco Security Agent ルールの作成」（P.2-8）
- 「Internet Explorer の信頼済みサイト リストに対する ASA の追加（Vista および Windows 7）」（P.2-9）
- 「ブラウザの警告ウィンドウに対応するセキュリティ証明書の追加」（P.2-9）
- 「複数の AnyConnect イメージをロードする場合の接続時間の短縮方法」（P.2-11）
- 「AnyConnect トラフィックに対するネットワーク アドレス変換（NAT）の免除」（P.2-11）
- 「非推奨の DES-only SSL 暗号化用 ASA 設定」（P.2-17）
- 「3G カードとの接続」（P.2-17）

証明書に関するユーザ プロンプトを最小限にする

AnyConnect のセットアップ中のユーザへのプロンプトを最小限にするには、次のようにクライアント PC と ASA の証明書データを一致させます。

- ASA 上の証明書に対して Certificate Authority（CA; 認証局）を使用する場合は、クライアント マシンで信頼済み CA として設定された証明書を選択します。
- ASA 上の自己署名証明書を使用するか、自社内の証明書サーバで生成した証明書を使用する会社の場合は、必ず、信頼できるルート証明書として証明書をクライアントにインストールしてください。

  手順はブラウザによって異なります。この項の次の手順を参照してください。
- VPN の確立に先立って、エンドポイントから認証局および内部証明書サーバに到達可能である必要があります。
- ASA 証明書の Common Name（CN; 通常名）と、AnyConnect が接続に使用する名前が一致していることを確認します。デフォルトでは、ASA 証明書の CN フィールドは IP アドレスになっています。AnyConnect が DNS 名を使用する場合は、ASA 証明書の CN フィールドをその名前に変更します。

  証明書に SAN（Subject Alternate Name）が含まれている場合、ブラウザは [件名（Subject）] フィールドの CN 値を無視し、[SAN] フィールドの [DNS 名（DNS Name）] エントリを調べます。

  ユーザがホスト名を使用して ASA に接続する場合は、SAN に ASA のホスト名とドメイン名が含まれている必要があります。たとえば、SAN フィールドには次が含まれます。
  `DNS Name=hostname.domain.com`.

  ユーザが IP アドレスを使用して ASA に接続する場合は、SAN に ASA の IP アドレスが含まれている必要があります。たとえば、SAN フィールドには `DNS Name=209.165.200.254` と入力されます。

AnyConnect 用 Cisco Security Agent ルールの作成

AnyConnect のインストール中に、Cisco Security Agent（CSA）から警告が表示されることがあります。

現在出荷中の CSA バージョンには、AnyConnect と互換性のある組み込みルールがありません。CSA バージョン 5.0 以降を使用すると、次の手順により次のルールを作成できます。

ステップ 1　ルール モジュール「Cisco Secure Tunneling Client Module」で次の FACL を追加します。

```
Priority Allow, no Log, Description: "Cisco Secure Tunneling Browsers, read/write
vpnweb.ocx"
Applications in the following class: "Cisco Secure Tunneling Client - Controlled Web
Browsers"
Attempt: Read file, Write File
```

すべての @SYSTEM\vpnweb.ocx ファイルで、次のことを行います。

ステップ 2　アプリケーション クラス :「Cisco Secure Tunneling Client - Installation Applications」に次のプロセス名を追加します。

```
**\vpndownloader.exe
@program_files\**\Cisco\Cisco AnyConnect Secure Mobility Client\vpndownloader.exe
```

Internet Explorer の信頼済みサイト リストに対する ASA の追加（Vista および Windows 7）

Microsoft Internet Explorer（MSIE）ユーザは、信頼済みサイト リストに ASA を追加するか、Java をインストールすることをお勧めします。信頼済みサイト リストに追加すると、ActiveX コントロールで、最小限のユーザ操作によるインストールが可能になります。セキュリティが強化された Windows XP SP2 のユーザにとって、この推奨事項は特に重要です。

Vista ユーザおよび Windows 7 ユーザの場合は、AnyConnect クライアントを展開する ASA が、ユーザ コンピュータ上の信頼済みサイトのリストにある必要があります。そうでない場合は、WebLaunch は起動しません。

ユーザは、次の手順を実行することにより、Microsoft Internet Explorer の信頼済みサイト リストに ASA を追加できます。

（注）　これは、Windows Vista および Windows 7 で WebLaunch を使用するために必要です。

ステップ 1　[ツール（Tools）] > [インターネット オプション（Internet Options）] を選択します。[インターネット オプション（Internet Options）] ウィンドウが開きます。

ステップ 2　[セキュリティ（Security）] タブをクリックします。

ステップ 3　[信頼されたサイト（Trusted Sites）] アイコンをクリックします。

ステップ 4　[サイト（Sites）] をクリックします。[信頼されたサイト（Trusted Sites）] ウィンドウが開きます。

ステップ 5　ASA のホスト名または IP アドレスを入力します。複数のサイトをサポートするため、https://*.yourcompany.com のようなワイルドカードを使用して、yourcompany.com ドメイン内のすべての ASA 5500 が使用できるようにします。

ステップ 6　[追加（Add）] をクリックします。

ステップ 7　[OK] をクリックします。[信頼されたサイト（Trusted Sites）] ウィンドウが閉じます。

ステップ 8　[インターネット オプション（Internet Options）] ウィンドウで [OK] をクリックします。

ブラウザの警告ウィンドウに対応するセキュリティ証明書の追加

ここでは、ブラウザの警告ウィンドウへの対応として、自己署名証明書を信頼済みルート証明書としてクライアントにインストールする方法について説明します。

Microsoft Internet Explorer の [セキュリティ アラート（Security Alert）] ウィンドウへの対応

ここでは、Microsoft Internet Explorer の [セキュリティ アラート（Security Alert）] ウィンドウへの対応として、自己署名証明書を信頼済みルート証明書としてクライアントにインストールする方法について説明します。このウィンドウは、Microsoft Internet Explorer で、信頼済みサイトとして認識されない ASA への接続が確立するときに開きます。[セキュリティ アラート（Security Alert）] ウィンドウの上半分には、次のテキストが表示されます。

```
Information you exchange with this site cannot be viewed or changed by others.However,
there is a problem with the site's security certificate.The security certificate was
issued by a company you have not chosen to trust.View the certificate to determine
whether you want to trust the certifying authority.
```

次の手順にしたがって、信頼済みルート証明書として証明書をインストールします。

ステップ 1　[セキュリティの警告（Security Alert）] ウィンドウの [証明書の表示（View Certificate）] をクリックします。[証明書（Certificate）] ウィンドウが開きます。

ステップ 2　[証明書のインストール（Install Certificate）] をクリックします。[証明書インポート ウィザード ようこそ（Certificate Import Wizard Welcome）] が開きます。

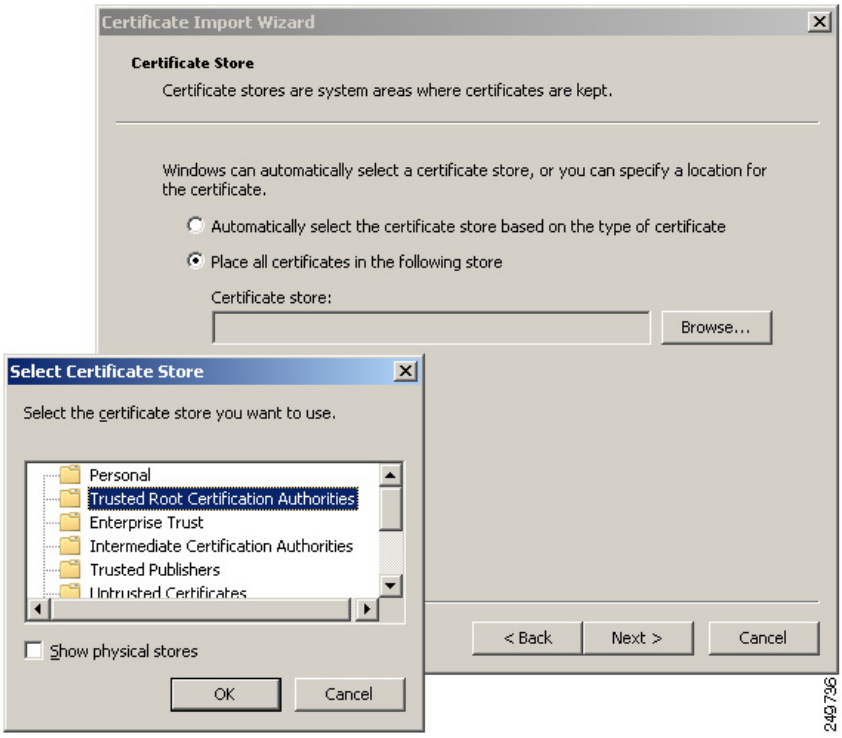
ステップ 3　[次へ（Next）] をクリックします。[証明書インポート ウィザード - 証明書ストア（Certificate Import Wizard - Certificate Store）] ウィンドウが開きます。

ステップ 4　[すべての証明書を次のストアに配置する（Place all certificates in the following store）] を選択します。

ステップ 5　[参照（Browse）] をクリックします。[証明書ストアの選択（Select Certificate Store）] ウィンドウが開きます。

ステップ 6　ドロップダウン リストで、[信頼済みルート認証局（Trusted Root Certification Authorities）] を選択します（図 2-3 を参照）。

図 2-3　　証明書のインポート



ステップ 7　[次へ（Next）] をクリックします。[証明書インポート ウィザード - 完了（Certificate Import Wizard - Completing）] ウィンドウが開きます。

ステップ 8　[完了（Finish）] をクリックします。別の [セキュリティ上の警告（Security Warning）] ウィンドウで「Do you want to install this certificate?」というメッセージが表示されます。

ステップ 9　[はい（Yes）] をクリックします。[証明書インポート ウィザード（Certificate Import Wizard）] ウィンドウに、インポートが成功したというメッセージが表示されます。

ステップ 10　[OK] をクリックして、このウィンドウを閉じます。

ステップ 11　[OK] をクリックして、[証明書（Certificate）] ウィンドウを閉じます。

ステップ 12　[はい（Yes）] をクリックして、[セキュリティ アラート（Security Alert）] ウィンドウを閉じます。ASA のウィンドウが開き、証明書が信頼されたというメッセージが表示されます。

Netscape、Mozilla、または Firefox の [不明な認証局により認証済み（Certified by an Unknown Authority）] ウィンドウへの対応

ここでは、[不明な認証局により認証された Web サイト（Web Site Certified by an Unknown Authority）] ウィンドウへの対応として、自己署名証明書を信頼済みルート証明書としてクライアントにインストールする方法について説明します。このウィンドウは、Netscape、Mozilla、または Firefox で、信頼済みサイトとして認識されない ASA への接続が確立するときに開きます。このウィンドウには、次のテキストが表示されます。

```
Unable to verify the identity of <Hostname_or_IP_address> as a trusted site.
```

次の手順にしたがって、信頼済みルート証明書として証明書をインストールします。

ステップ 1　[不明な認証局により認証された Web サイト（Web Site Certified by an Unknown Authority）] ウィンドウの [証明書の検証（Examine Certificate）] をクリックします。[証明書ビューア（Certificate Viewer）] ウィンドウが開きます。

ステップ 2　[この証明書を常に承認する（Accept this certificate permanently）] オプションをクリックします。

ステップ 3　[OK] をクリックします。ASA のウィンドウが開き、証明書が信頼されたというメッセージが表示されます。

複数の AnyConnect イメージをロードする場合の接続時間の短縮方法

複数の AnyConnect イメージを ASA にロードする場合は、リモート ユーザ数が最大のときに接続時間が最短になる順序で、イメージをロードする必要があります。

セキュリティ アプライアンスは、オペレーティング システムと一致するまで、AnyConnect イメージの一部をリモート コンピュータにダウンロードします。イメージのダウンロードは、リストの上から順に行われます。そのため、リモート コンピュータで最も頻繁に使用されているオペレーティング システムと一致するイメージを、リストの先頭に指定する必要があります。

AnyConnect トラフィックに対するネットワーク アドレス変換（NAT）の免除

ネットワーク アドレス変換（NAT）を実行するように ASA を設定してある場合は、AnyConnect クライアントのトラフィックを変換から除外して、AnyConnect クライアント、内部ネットワーク、DMZ 上のエンタープライズ リソースが、相互にネットワーク接続を開始できるようにする必要があります。AnyConnect クライアント トラフィックを変換の対象外にできないと、AnyConnect クライアントおよび他の企業リソースが通信できなくなります。

「アイデンティティ NAT」（「NAT」免除とも呼ばれている）によりアドレスを自らに変換できます。これにより効果的に NAT が回避されます。アイデンティティ NAT は 2 つのアドレス プール、アドレス プールとサブネットワーク、または 2 つのサブネットワーク間で適用できます。

この手順は、例にあるネットワーク トポロジの次の仮定のネットワーク オブジェクト間でアイデンティティ NAT を設定する方法を示しています。それらは、Engineering VPN アドレス プール、Sales VPN アドレス プール、ネットワーク内、DMZ ネットワーク、およびインターネットです。アイデンティティ NAT 設定ではそれぞれ、NAT 規則が 1 つ必要です。

表 2-2　VPN クライアントのアイデンティティ NAT を設定するネットワーク アドレス アドレッシング

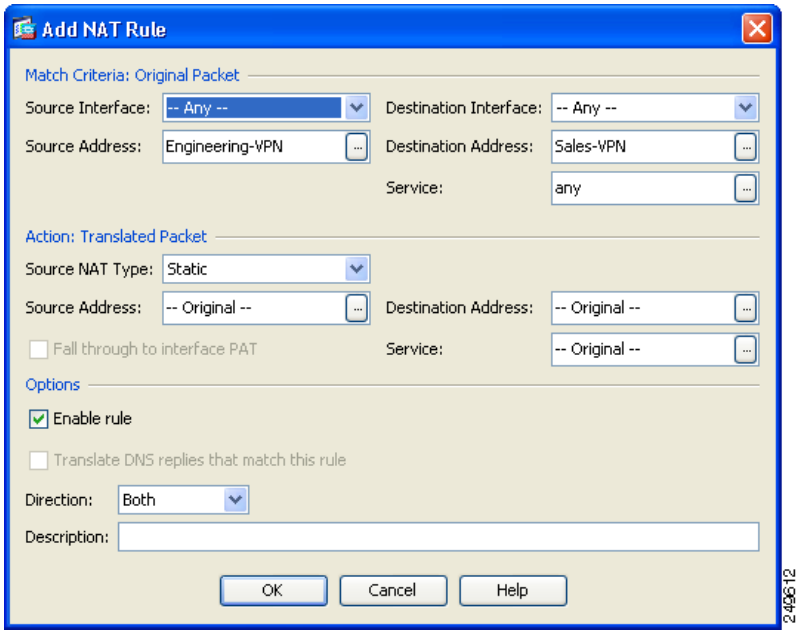
ネットワークまたはアドレス プール	ネットワーク名またはアドレス プール名	アドレス範囲
内部ネットワーク	inside-network	10.50.50.0 - 10.50.50.255
Engineering VPN アドレス プール	Engineering-VPN	10.60.60.1 - 10.60.60.254
Sales VPN アドレス プール	Sales-VPN	10.70.70.1 - 10.70.70.254
DMZ ネットワーク	DMZ-network	192.168.1.0 - 192.168.1.255

ステップ 1　ASDM にログインし、[設定（Configuration）] > [ファイアウォール（Firewall）] > [NAT ルール（NAT Rules）] を選択します。

ステップ 2　Engineering VPN アドレス プールのホストが Sales VPN アドレス プールのホストに接続できるよう、NAT 規則を作成します。ASA が Unified NAT テーブルの他の規則の前にこの規則を評価するよう、[NAT ルール（NAT Rules）] ペインで、[追加（Add）] > [「ネットワーク オブジェクト」NAT ルールの前に NAT ルールを追加（Add NAT Rule Before "Network Object" NAT rules）] を選択します。[NAT ルールの追加（Add NAT rule）] ダイアログボックスの例については、図 2-4（P.2-12）を参照してください。

（注）　ASA ソフトウェア バージョン 8.3 では、NAT 規則の評価は上から下へ最初に一致したものに適用されます。いったんパケットが特定の NAT 規則と一致すると、それ以上評価は行われません。ASA が NAT 規則を早まって広範な NAT 規則に一致しないよう、Unified NAT テーブルの先頭に最も固有の NAT 規則を配置することが重要です。

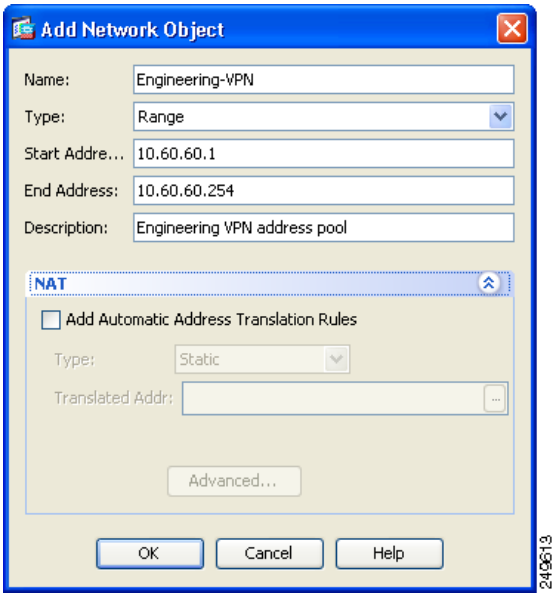
図 2-4　[NAT ルールの追加（Add NAT Rule）] ダイアログ ボックス



a.　[一致基準：元のパケット（Match criteria: Original Packet）] エリアで、次のフィールドを設定します。

- [送信元インターフェイス：（Source Interface:）] Any
- [宛先インターフェイス：（Destination Interface:）] Any
- [送信元アドレス：（Source Address:）] [送信元アドレス（Source Address）] ブラウズ ボタンをクリックし、Engineering VPN アドレス プールを表すネットワーク オブジェクトを作成します。オブジェクト タイプをアドレスの**範囲**として定義します。自動アドレス トランスレーション ルールは追加しないでください。例については、図 2-5 を参照してください。
- [宛先アドレス：（Destination Address:）] [宛先アドレス（Destination Address）] ブラウズ ボタンをクリックし、Sales VPN アドレス プールを表すネットワーク オブジェクトを作成します。オブジェクト タイプをアドレスの**範囲**として定義します。自動アドレス トランスレーション ルールは追加しないでください。

図 2-5　VPN アドレス プールのネットワーク オブジェクトの作成



b. [アクション：変換されたパケット（Action Translated Packet）] エリアで、次のフィールドを設定します。

- [送信元 NAT のタイプ：（Source NAT Type:）] Static
- [送信元アドレス：（Source Address:）] Original
- [宛先アドレス：（Destination Address:）] Original
- [サービス：（Service:）] Original

c. [オプション（Options）] エリアで、次のフィールドを設定します。

- [ルールの有効化（Enable rule）] をオンにします。
- [このルールに一致する DNS 応答を変換する（Translate DNS replies that match this rule）] をオフにするか、空にしておきます。
- [方向：（Direction:）] Both
- [説明：（Description:）] 規則の説明を入力します。

d. [OK] をクリックします。

e. [適用（Apply）] をクリックします。規則は図 2-7（P.2-17）の 「統合された NAT テーブル」の規則 1 のようになるはずです。

CLI の例：

```
nat source static Engineering-VPN Engineering-VPN destination static Sales-VPN
Sales-VPN
```

f. [送信（Send）] をクリックします。

ステップ 3　ASA が NAT を実行している場合、同じ VPN プール内の 2 つのホストが互いに接続できるよう、またはそれらのホストが VPN トンネル経由でインターネットに接続できるよう、[同一インターフェイスに接続している複数のホスト間のトラフィックを有効にする（Enable traffic between two or more hosts connected to the same interface）] オプションをイネーブルにする必要があります。これを行うには ASDM で、[設定（Configuration）] > [デバイス設定（Device Setup）] > [インターフェイス（Interfaces）] を選択します。[インターフェイス（Interface）] パネルの下の [同一インターフェイスに接続している複数のホスト間のトラフィックを有効にする（Enable traffic between two or more hosts connected to the same interface）] をオンにし、[適用（Apply）] をクリックします。

CLI の例：

```
same-security-traffic permit inter-interface
```

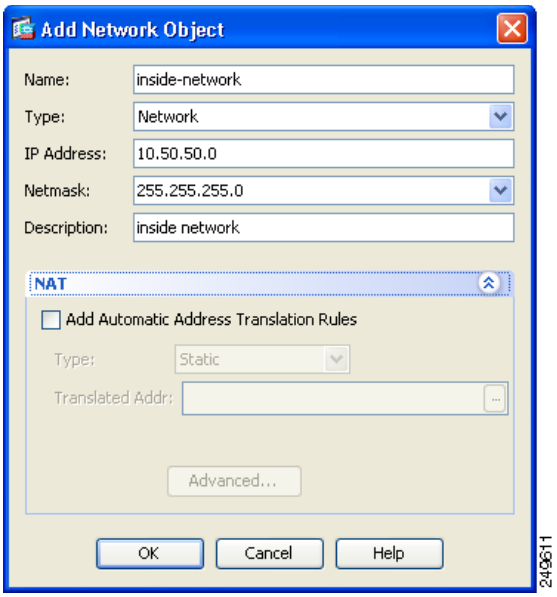
ステップ 4　Engineering VPN アドレス プールのホストが Engineering VPN アドレス プールの他のホストに接続できるよう、NAT 規則を作成します。ステップ 2 で規則を作成したときのようにこの規則を作成します。ただし、[一致基準：元のパケット（Match criteria: Original Packet）] エリアで Engineering VPN アドレス プールを送信元アドレスおよび宛先アドレス両方として指定します。

ステップ 5　Engineering VPN リモート アクセス クライアントが「内部」ネットワークに接続できるよう NAT 規則を作成します。この規則が他の規則の前に処理されるよう [NAT ルール（NAT Rules）] ペインで、[追加（Add）] > [「ネットワーク オブジェクト」NAT ルールの前に NAT ルールを追加（Add NAT Rule Before "Network Object" NAT rules）] を選択します。

a. [一致基準：元のパケット（Match criteria: Original Packet）] エリアで、次のフィールドを設定します。

- [送信元インターフェイス：（Source Interface:）] Any
- [宛先インターフェイス：（Destination Interface:）] Any
- [送信元アドレス：（Source Address:）] [送信元アドレス（Source Address）] ブラウズ ボタンをクリックし、内部ネットワークを表すネットワーク オブジェクトを作成します。オブジェクト タイプをアドレスの**ネットワーク**として定義します。自動アドレス トランスレーション ルールは追加しないでください。
- [宛先アドレス：（Destination Address:）] [宛先アドレス（Destination Address）] ブラウズ ボタンをクリックし、Engineering VPN アドレス プールを表すネットワーク オブジェクトを選択します。

図 2-6　inside-network オブジェクトの追加



b. [アクション：変換されたパケット（Action Translated Packet）] エリアで、次のフィールドを設定します。

- [送信元 NAT のタイプ：（Source NAT Type:）] Static
- [送信元アドレス：（Source Address:）] Original
- [宛先アドレス：（Destination Address:）] Original
- [サービス：（Service:）] Original

c. [オプション（Options）] エリアで、次のフィールドを設定します。

- [ルールの有効化（Enable rule）] をオンにします。
- [このルールに一致する DNS 応答を変換する（Translate DNS replies that match this rule）] をオフにするか、空にしておきます。
- [方向：（Direction:）] Both
- [説明：（Description:）] 規則の説明を入力します。

d. [OK] をクリックします。

e. [適用（Apply）] をクリックします。規則は図 2-7（P.2-17）の 「統合された NAT テーブル」の規則 2 のようになるはずです。

CLI の例

```
nat source static inside-network inside-network destination static Engineering-VPN
Engineering-VPN
```

ステップ 6　ステップ 5 の方法にしたがって新しい規則を作成し、Engineering VPN アドレス プールと DMZ ネットワーク間の接続のアイデンティティ NAT を設定します。DMZ ネットワークを送信元アドレス、Engineering VPN アドレス プールを宛先アドレスとして使用します。

ステップ 7　新しい NAT 規則を作成して、Engineering VPN アドレス プールをトンネル経由にインターネットにアクセスできるようにします。この場合、アイデンティティ NAT は使用しません。送信元アドレスをプライベート アドレスからインターネット ルーティング可能なアドレスに変更するためです。この規則を作成するには、次の手順に従います。

a. この規則が他の規則の前に処理されるよう [NAT ルール（NAT Rules）] ペインで、[追加（Add）] > [「ネットワーク オブジェクト」NAT ルールの前に NAT ルールを追加（Add NAT Rule Before "Network Object" NAT rules）] を選択します。

b. [一致基準：元のパケット（Match criteria: Original Packet）] エリアで、次のフィールドを設定します。

- [送信元インターフェイス：（Source Interface:）] Any
- [宛先インターフェイス：（Destination Interface:）] Any [アクション：変換されたパケット（Action: Translated Packet）] エリアの [送信元アドレス（Source Address）] に [外部（outside）] を選択すると、このフィールドには自動的に「outside」が入力されます。
- [送信元アドレス：（Source Address:）] [送信元アドレス（Source Address）] ブラウズ ボタンをクリックし、Engineering VPN アドレス プールを表すネットワーク オブジェクトを選択します。
- [宛先アドレス：（Destination Address:）] Any

c. [アクション：変換されたパケット（Action Translated Packet）] エリアで、次のフィールドを設定します。

- [送信元 NAT のタイプ：（Source NAT Type:）] Dynamic PAT (Hide)
- [送信元アドレス：（Source Address:）] [送信元アドレス（Source Address）] ブラウズ ボタンをクリックし、outside インターフェイスを選択します。
- [宛先アドレス：（Destination Address:）] Original
- [サービス：（Service:）] Original

d. [オプション（Options）] エリアで、次のフィールドを設定します。

- [ルールの有効化（Enable rule）] をオンにします。
- [このルールに一致する DNS 応答を変換する（Translate DNS replies that match this rule）] をオフにするか、空にしておきます。
- [方向：（Direction:）] Both
- [説明：（Description:）] 規則の説明を入力します。

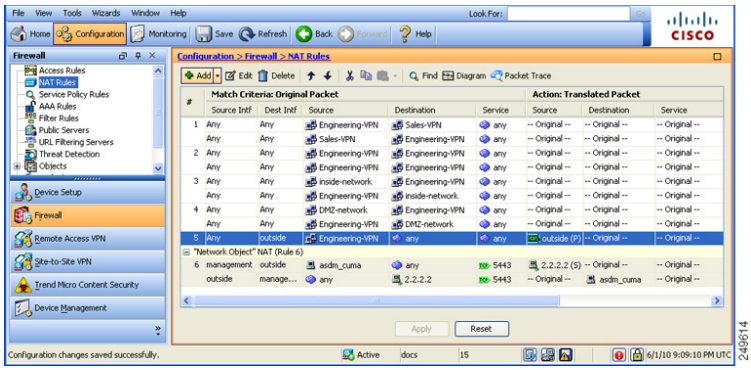
e. [OK] をクリックします。

f. [適用（Apply）] をクリックします。規則は図 2-7（P.2-17）の 「統合された NAT テーブル」の規則 5 のようになるはずです。

CLI の例：

```
nat (any,outside) source dynamic Engineering-VPN interface
```

図 2-7　統合された NAT テーブル



ステップ 8　Engineering VPN アドレス プール、Sales VPN アドレス プール、内部ネットワーク、DMZ ネットワーク、およびインターネットに接続するように Engineering VPN アドレス プールを設定した後で、Sales VPN アドレス プールについて、同じプロセスを繰り返す必要があります。アイデンティティ NAT を使用して、Sales VPN アドレス プール トラフィックが、Sales VPN アドレス プール、内部ネットワーク、DMZ ネットワーク、およびインターネット間のネットワーク アドレス変換の対象外となるようにします。

ステップ 9　ASA の [ファイル（File）] メニューで [実行コンフィギュレーションをフラッシュに保存する（Save Running Configuration to Flash）] を選択し、アイデンティティ NAT 規則を実装します。

非推奨の DES-only SSL 暗号化用 ASA 設定

Windows Vista および Windows 7 は、デフォルトでは、DES SSL 暗号化をサポートしません。ASA に DES-only を設定した場合、AnyConnect 接続は失敗します。これらのオペレーティング システムの DES 対応設定は難しいため、ASA には、DES のみの SSL 暗号化を設定しないことをお勧めします。

3G カードとの接続

一部の 3G カードには、AnyConnect に接続する前に必要な、設定手順があります。たとえば、Verizon Access Manager には、次の 3 つの設定があります。

- modem manually connect
- modem auto connect except when roaming
- lan adapter auto connect

[lan adapter auto connect] を選択した場合は、プリファレンスを NDIS モードに設定できます。NDIS は、VZAccess Manager が終了されても接続を続行できる、常時接続です。VZAccess Manager では、AnyConnect インストールの準備ができると、自動接続 LAN アダプタをデバイス接続のプリファレンスとして表示します。AnyConnect インターフェイスが検出されると、3G マネージャはインターフェイスをドロップし、AnyConnect 接続を許可します。

AnyConnect をダウンロードするための ASA の設定

AnyConnect の Web 展開用に ASA を準備するには、次の手順を実行します。

ステップ 1　「AnyConnect の正常インストールの確認」（P.2-7）の手順を確認して、自社に該当する手順を実行します。

ステップ 2　Cisco AnyConnect Software Download の Web ページから最新の Cisco AnyConnect Secure Mobility Client パッケージをダウンロードします。AnyConnect ファイル パッケージのリストについては、「ASA 展開用の AnyConnect ファイル パッケージ」（P.2-7）を参照してください。

ステップ 3　Cisco AnyConnect Secure Mobility Client パッケージ ファイルをクライアント イメージとして指定します。[設定（Configuration）] > [リモート アクセス VPN（Remote Access VPN）] > [ネットワーク（クライアント）アクセス（Network (Client) Access）] > [AnyConnect クライアント設定（AnyConnect Client Settings）] に移動します。AnyConnect イメージとして指定されたクライアント ファイルをリストした、[AnyConnect クライアント設定（AnyConnect Client Settings）] パネルが表示されます（図 2-8）。表示順序は、ASA によるリモート コンピュータへのダウンロード順序を示しています。

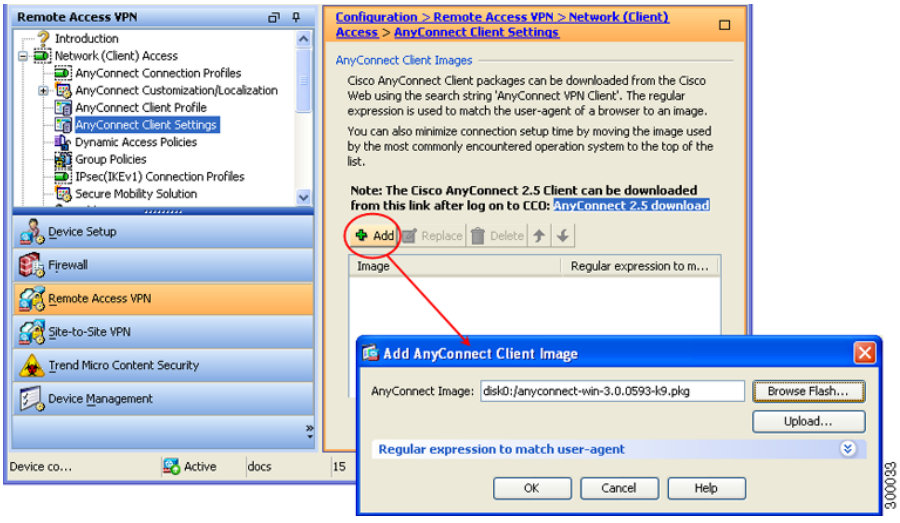
ステップ 4　AnyConnect イメージを追加するには、[AnyConnect クライアント イメージ（AnyConnect Client Images）] エリアで [追加（Add）] をクリックします。

- ASA にアップロードした AnyConnect イメージを選択するには、[フラッシュの参照（Browse Flash）] をクリックします。
- コンピュータ上にローカルに保存した AnyConnect イメージを参照して選択するには、[アップロード（Upload）] をクリックします。

ステップ 5　[OK] または [アップロード（Upload）] をクリックします。

ステップ 6　[適用（Apply）] をクリックします。

図 2-8　AnyConnect イメージの指定

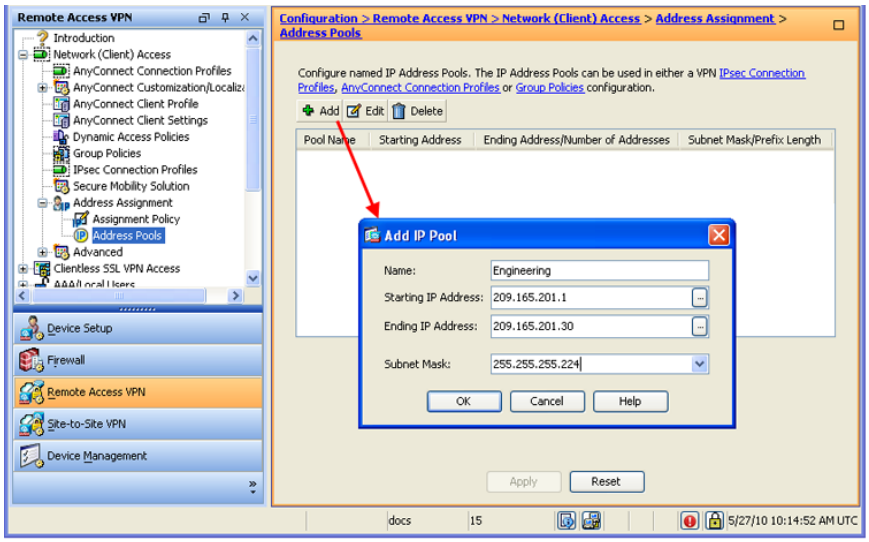


ステップ 7　アドレスの割り当て方式を設定します。

DHCP や、ユーザが割り当てたアドレス指定を使用できます。ローカル IP アドレス プールを作成し、そのプールを接続プロファイルに割り当てる方法もあります。このガイドでは、一般的なアドレス プール方式を例として使用します。

[設定（Configuration）] > [リモート アクセス VPN（Remote Access VPN）] > [ネットワーク（クライアント）アクセス（Network (Client) Access）] > [アドレス割り当て（Address Assignment）] > [アドレス プール（Address Pools）] を選択します（図 2-9）。[IP プールの追加（Add IP Pool）] ウィンドウにアドレス プール情報を入力します。

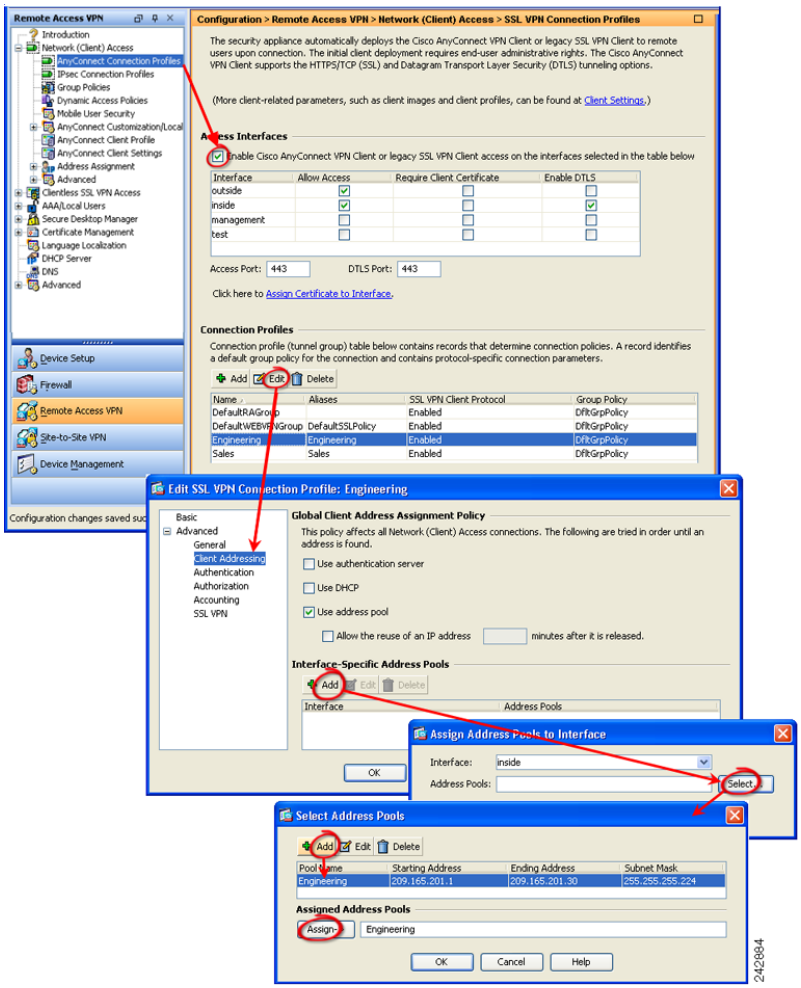
図 2-9　[IP プールの追加（Add IP Pool）] ダイアログ



ステップ 8　AnyConnect のダウンロードをイネーブルにし、接続プロファイルのアドレス プールを割り当てます。

[設定（Configuration）] > [リモート アクセス VPN（Remote Access VPN）] > [ネットワーク（クライアント）アクセス（Network (Client) Access）] > [AnyConnect 接続プロファイル（AnyConnect Connection Profiles）] を選択します。（図 2-10）の矢印に従って AnyConnect クライアントをイネーブルにしてから、アドレス プールを割り当てます。

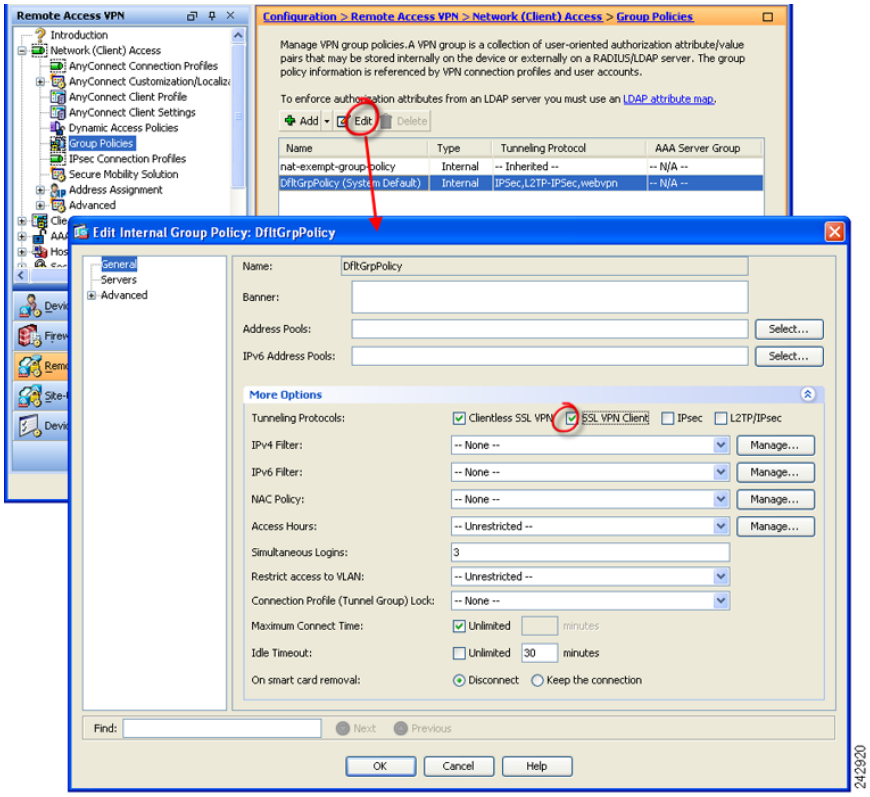
図 2-10　AnyConnect のダウンロードのイネーブル化



ステップ 9　グループ ポリシーで許可された VPN トンネリング プロトコルとして SSL VPN クライアントを指定します。

[設定（Configuration）] > [リモート アクセス VPN（Remote Access VPN）] > [ネットワーク（クライアント）アクセス（Network (Client) Access）] > [グループ ポリシー（Group Policies）] を選択します。[グループ ポリシー（Group Policies）] パネルが表示されます。図 2-11 の矢印に従って、グループの SSL VPN クライアントをイネーブルにします。

図 2-11　トンネリング プロトコルとしての SSL VPN の指定



リモート ユーザへの AnyConnect ダウンロードの要求

リモート ユーザが最初にブラウザで接続している場合、デフォルトでは ASA は AnyConnect をダウンロードしません。ユーザの認証後、デフォルトのクライアントレス ポータル ページに [Start AnyConnect Client] ドロワーが表示され、ユーザが AnyConnect のダウンロードを選択できるようになっています。または、クライアントレス ポータル ページを表示することなく、すぐに AnyConnect をダウンロードするよう ASA を設定できます。

リモート ユーザにプロンプトを表示し、設定された時間内に AnyConnect をダウンロードするか、クライアントレス ポータル ページを表示するよう ASA を設定することもできます。

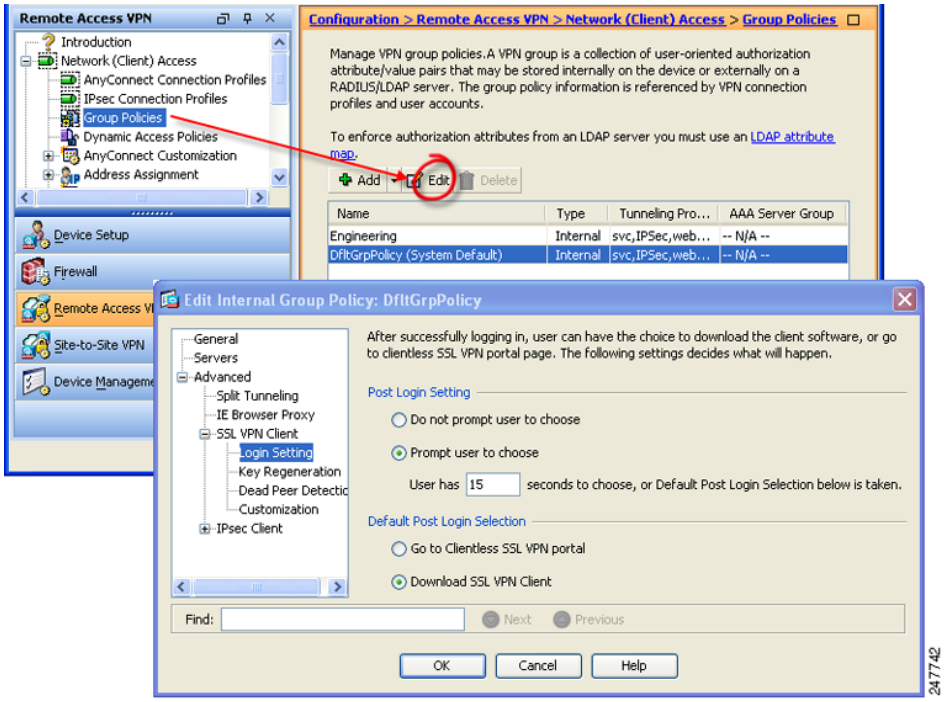
この機能は、グループ ポリシーまたはユーザに対して設定できます。このようなログイン設定を変更するには、次の手順に従ってください。

ステップ 1　[設定（Configuration）] > [リモート アクセス VPN（Remote Access VPN）] > [ネットワーク（クライアント）アクセス（Network (Client) Access）] > [グループ ポリシー（Group Policies）] を選択します。グループ ポリシーを選択して、[編集（Edit）] をクリックします。[内部グループ ポリシーの編集（Edit Internal Group Policy）] ウィンドウが表示されます（図 2-12）。

ステップ 2　ナビゲーション ペインで、[詳細（Advanced）] > [AnyConnect クライアント（AnyConnect Client）] > [ログイン設定（Login Settings）] を選択します。[ログイン後の設定（Post Login settings）] が表示されます。必要に応じて [継承（Inherit）] チェックボックスをオフにし、[ログイン後の設定（Post Login setting）] を選択します。

ユーザにプロンプトを表示する場合は、タイムアウト時間を指定し、その時間経過後のデフォルト動作を [Default Post Login Selection] エリアで選択します。

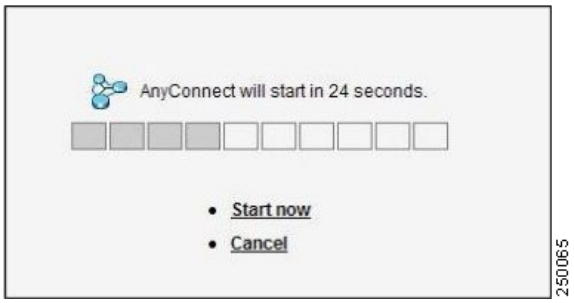
図 2-12　ログイン設定の変更



ステップ 3　[OK] をクリックし、変更をグループ ポリシーに適用します。

図 2-13 は、[Prompt user to choose] と [SSL VPN クライアントのダウンロード（Download SSL VPN Client）] を選択した場合に、リモート ユーザに表示されるプロンプトを示しています。

図 2-13　リモート ユーザに表示されるログイン後プロンプト



追加機能で使用するモジュールのイネーブル化

AnyConnect で機能をイネーブルにすると、新機能を使用するため VPN エンドポイントのモジュールを更新する必要があります。ダウンロード時間を最小限に抑えるため、AnyConnect は、サポートされる各機能に必要なモジュールだけ（ASA から）ダウンロードするよう要求します。

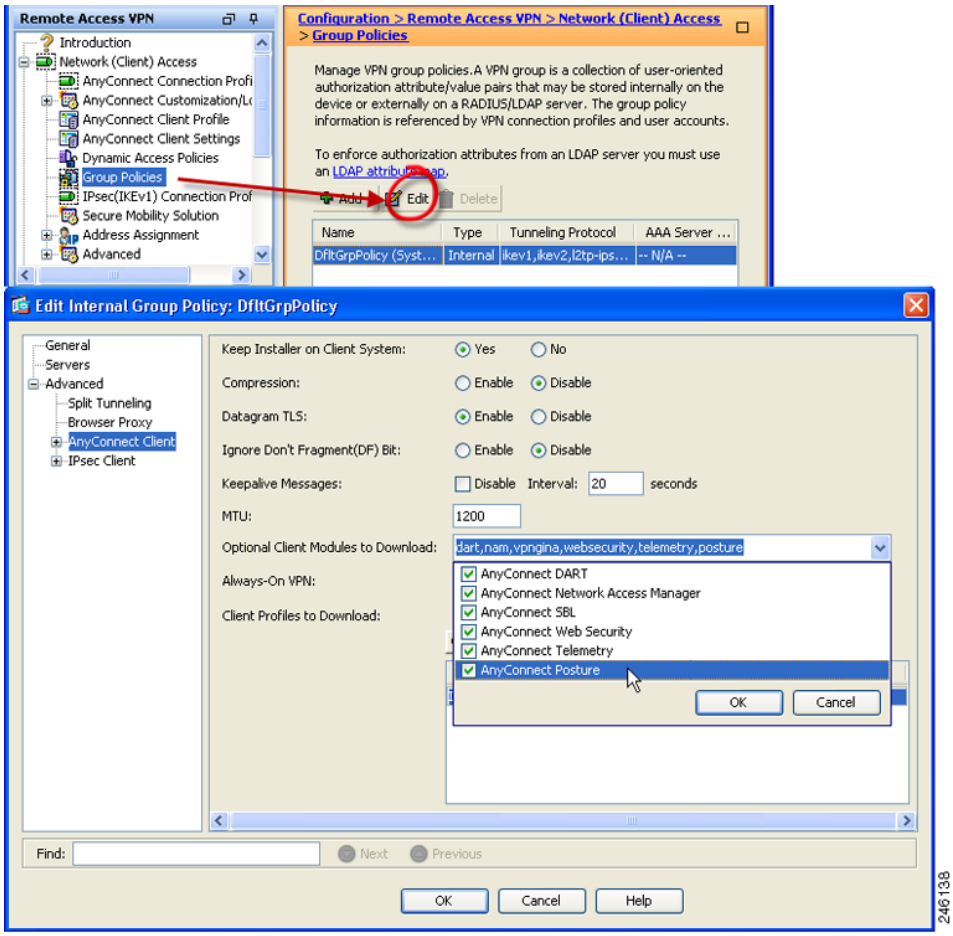
新機能をイネーブルにするには、グループ ポリシーまたはユーザ名の設定の一部として、新しいモジュール名を指定する必要があります。グループ ポリシーのモジュール ダウンロードをイネーブルにするには、次の手順に従います。

ステップ 1　[設定（Configuration）] > [リモート アクセス VPN（Remote Access VPN）] > [ネットワーク（クライアント）アクセス（Network (Client) Access）] > [グループ ポリシー（Group Policies）] を選択します。グループ ポリシーを選択して、[編集（Edit）] をクリックします。[内部グループ ポリシーの編集（Edit Internal Group Policy）] ウィンドウが表示されます（図 2-14）。

ステップ 2　ナビゲーション ペインで、[詳細（Advanced）] > [AnyConnect クライアント（AnyConnect Client）] を選択します。 [ダウンロードするオプションのクライアント モジュール（Optional Client Module to Download）] ドロップリストをクリックし、モジュールを選択します。

- AnyConnect DART：DART をダウンロードすると、AnyConnect のインストールと収集に関する問題のトラブルシューティングに有用なデータを収集できます。
- AnyConnect ネットワーク アクセス マネージャ：このモジュールにより、最適なレイヤ 2 アクセス ネットワークの検出と選択ができ、有線とワイヤレスの両方のネットワークにアクセスするためのデバイス認証を実行できます。
- AnyConnect SBL：Start Before Logon（SBL）モジュールは、Windows のログイン ダイアログ ボックスが表示される前に AnyConnect を開始することにより、ユーザを Windows へのログイン前に企業インフラへ強制的に接続させます。SBL をイネーブルにするさまざまな理由については、「Start Before Logon の設定」（P.3-7）を参照してください。
- AnyConnect Web セキュリティ：Web セキュリティは、HTTP トラフィックを ScanSafe スキャニング プロキシにルーティングするエンドポイント コンポーネントです。トラフィックは、プロキシ上で ScanSafe Web スキャニング サービスによって評価されます。
- AnyConnect テレメトリ：テレメトリ モジュールは、悪意のあるコンテンツの発信元に関する情報を Cisco IronPort Web セキュリティ アプライアンス（WSA）の Web フィルタリング インフラストラクチャに送信します。
- AnyConnect ポスチャ：ポスチャ モジュールにより、クライアントでは、ホストにインストールされているオペレーティング システム、アンチウイルス、アンチスパイウェア、ファイアウォールの各ソフトウェアを識別できます。

図 2-14　ダウンロードするオプションのクライアント モジュールの指定



ステップ 3　[OK] をクリックし、変更をグループ ポリシーに適用します。

（注）　[ログイン前の起動（Start Before Logon）] を選択した場合は、AnyConnect クライアント プロファイルでもこの機能をイネーブルにする必要があります。詳細については、「」第 3 章「VPN アクセスの設定」を参照してください。

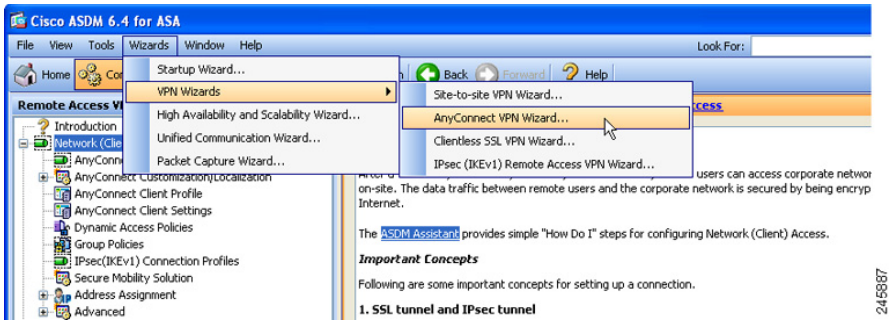
IPsec IKEv2 接続のイネーブル化

ここでは、ASA 上で IPsec IKEv2 接続をイネーブルにする手順を示します。

AnyConnect クライアント パッケージを ASA にロードした後で、次の手順を実行して、ASA に IPsec IKEv2 接続を設定します。

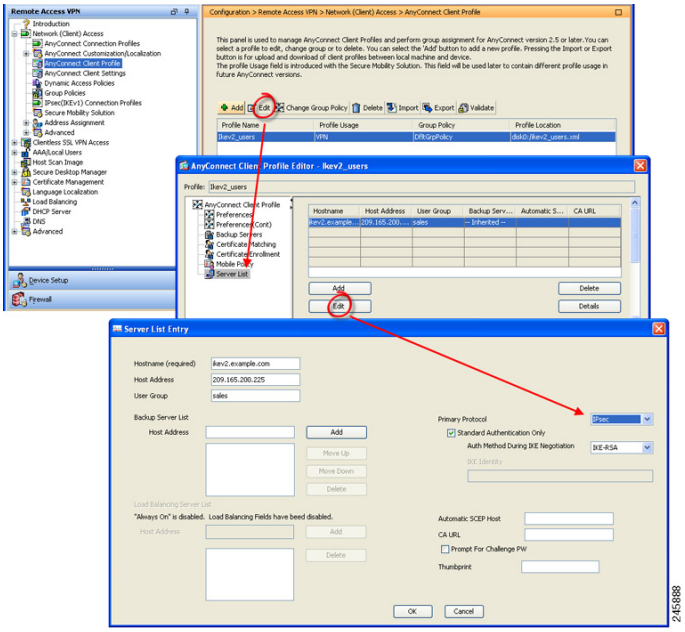
ステップ 1　AnyConnect VPN Wizard を実行します。[ツール（Tools）] > [ウィザード（Wizards）] > [AnyConnect VPN Wizard] を選択します（図 2-15）。ウィザードの手順に従って、IPsec IKEv2 接続用の基本 VPN 接続を作成します。

図 2-15　AnyConnect VPN Wizard



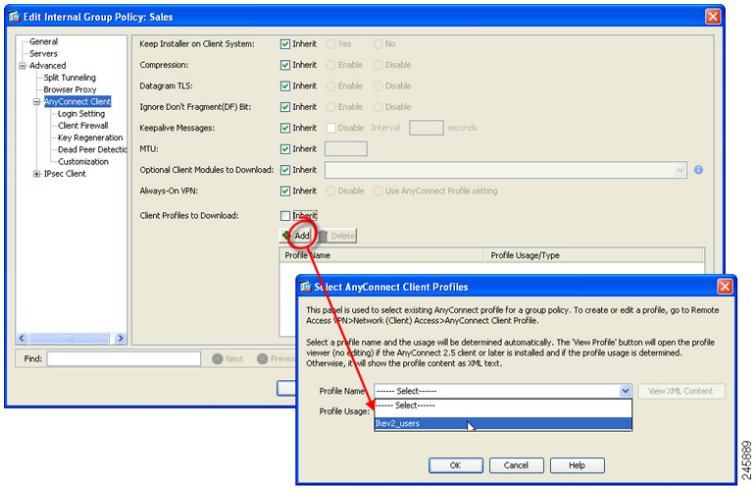
ステップ 2　プロファイル エディタを使用して、VPN プロファイルの [サーバ リスト（Server List）] エントリを編集します。[設定（Configuration）] > [リモート アクセス VPN（Remote Access VPN）] > [ネットワーク（クライアント）アクセス（Network (Client) Access）] > [AnyConnect クライアント プロファイル（AnyConnect Client Profile）] を選択します（図 2-16）。

図 2-16　AnyConnect クライアント プロファイルでの IKEv2 の指定



ステップ 3　VPN プロファイルを、使用するグループ ポリシーと関連付けます。[設定（Configuration）] > [リモート アクセス VPN（Remote Access VPN）] > [ネットワーク（クライアント）アクセス（Network (Client) Access）] > [グループ ポリシー（Group Policies）] を選択します。グループ ポリシーを編集し、[詳細（Advanced）] > [AnyConnect クライアント（AnyConnect Client）] に移動します（図 2-17）。

図 2-17　プロファイルとグループ ポリシーの関連付け



IKEv2-enabled クライアント プロファイルの事前展開

ソフトウェア管理システムを使用してクライアントを事前展開するときは、IKEv2-enabled クライアント プロファイルも事前展開する必要があります。手順は次のとおりです。

ステップ 1　Winzip、7-zip、または同様のユーティリティを使用して、.ISO を解凍します。

ステップ 2　次のフォルダを参照して選択します。

anyconnect-win-3.0.0xxx-pre-deploy-k9\Profiles\vpn

ステップ 3　プロファイル エディタ（ASDM バージョンまたはスタンドアロン バージョン）を使用して作成した IKEv2/IPSec VPN プロファイルを、次のフォルダにコピーします。

ステップ 4　Setup.exe を実行して、インストーラを実行し、[すべて選択（Select all）] をオフに、[AnyConnect VPN モジュール（AnyConnect VPN Module）] のみをオンにします。

仮想 CD マウント ソフトウェアによるクライアント プロファイルの事前展開

SlySoft、PowerISO などの仮想 CD マウント ソフトウェアを使用して、クライアント プロファイルを事前展開することもできます。手順は次のとおりです。

ステップ 1　仮想 CD マウント ソフトウェアを使用して、.ISO をマウントします。

ステップ 2　ソフトウェアのインストール後、プロファイルを適切なフォルダに展開します（表 2-3 を参照）。

表 2-3　クライアントの展開先パス

OS	ディレクトリ パス
Windows 7 および Vista	C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\Profile\
Windows XP	C:\Document and Settings\All Users\Application Data\Cisco\Cisco AnyConnect Secure Mobility Client\Profile
Mac OS X および Linux	/opt/cisco/anyconnect/profile/

（注）　前のリリースの AnyConnect では、AnyConnect コンポーネントはパス /opt/cisco/vpn にインストールされました。現在、AnyConnect コンポーネントは、パス /opt/cisco/anyconnect にインストールされます。

事前展開に関するその他のヒント

MSI インストーラを使用する場合、MSI では、クライアント プロファイル（Profiles@@pl\vpn フォルダ）に配置されている任意のプロファイルを選択し、インストール中に適切なフォルダに配置します。

インストール後にプロファイルを手動で事前展開する場合は、手動か、Altiris などの SMS を使用してプロファイルをコピーすることにより、適切なフォルダにプロファイルを展開してください。

クライアントの Weblaunch

AnyConnect クライアントを Weblaunch するには、ASA の URL を次の形式でブラウザに入力して、ログインと AnyConnect クライアントのダウンロードを行うよう、ユーザに指示してください。

https://<asa>

AnyConnect クライアントおよびオプション モジュールの事前展開

ここでは、エンタープライズ ソフトウェア展開システムを使用してクライアントを展開するために必要な情報など、AnyConnect Secure Mobility Client の事前展開プロセスについて説明します。

以下の項では、AnyConnect クライアントを事前展開する方法について説明します。

事前展開パッケージ ファイル情報

AnyConnect VPN クライアントのコア モジュールおよびオプション モジュール（SBL、AnyConnect AnyConnect Diagnostic Reporting Tool など）は、独自のインストール ファイルまたはプログラムによってインストール、更新されます。AnyConnect バージョン 3.0 の場合、Windows デスクトップ インストール ファイルは、ISO イメージ（*.iso）に含まれています。その他のすべてのプラットフォームの場合は、AnyConnect バージョン 2.5 以前の場合と同じ方法で個々の任意のインストール ファイルを、任意の方法で個別に配布できます。

表 2-4 に、事前展開する AnyConnect パッケージのファイル名を OS ごとに示します。

表 2-4　事前展開する AnyConnect パッケージ ファイルの名前

OS	AnyConnect 3.0 事前展開パッケージ名
Windows	anyconnect-win-<*version*>-k9.iso
Mac OS X	anyconnect-macosx-i386-<*version*>-k9.dmg
Linux	anyconnect-linux-<*version*>-k9.tar.gz

Windows コンピュータへの事前展開

Windows コンピュータ（モバイルではなくデスクトップ）用の AnyConnect 3.0 事前展開インストールは、ISO イメージで配布されます。この ISO パッケージ ファイルは、*インストール ユーティリティ*、個々のコンポーネント インストーラを起動するセレクタ メニュー プログラム、AnyConnect のコア モジュールとオプション モジュール用の MSI を含みます。

以下の項では、Windows コンピュータに事前展開する方法について説明します。

- 「ISO ファイルの展開」（P.2-30）
- 「インストール ユーティリティのユーザへの展開」（P.2-30）
- 「Windows 用 AnyConnect モジュールで必要とされるインストールまたはアンインストール順序」（P.2-31）
- 「事前展開された AnyConnect モジュールのインストール」（P.2-32）
- 「ネットワーク アクセス マネージャおよび Web セキュリティをスタンドアロン アプリケーションとしてインストールするためのユーザ指示」（P.2-34）
- 「エンタープライズ ソフトウェア展開システム用 MSI ファイルのパッケージ化」（P.2-35）
- 「レガシー クライアントおよびオプション モジュールのアップグレード」（P.2-36）
- 「インストーラのカスタマイズとローカライズ」（P.2-36）

ISO ファイルの展開

事前展開パッケージは、ユーザ コンピュータに展開するプログラムおよび MSI インストーラ ファイルを含む ISO パッケージ ファイルにバンドルされています。ISO パッケージ ファイルを展開すると、セットアップ プログラム（setup.exe）によって、インストール ユーティリティ メニューが実行および展開されます。このメニューは、インストールする AnyConnect モジュールをユーザが選択できる、便利な GUI です。

必要に応じて、ISO イメージから個々のインストーラを取り出して、手動で配布することもできます。事前展開パッケージ内の各インストーラは、個別に実行できます。ファイルを展開する順序は、非常に重要です。詳細については、Windows 用 AnyConnect モジュールで必要とされるインストールまたは

アンインストール順序を参照してください。

表 2-5 に、ISO パッケージ ファイルを含んでいるファイルおよび各ファイルの目的を示します。

表 2-5　事前展開用 ISO ファイルの内容

ファイル	目的
GUI.ico	AnyConnect アイコン画像。
Setup.exe	インストール ユーティリティ（setup.hta）を起動します。
anyconnect-dart-win-<*version*>-k9.msi	DART オプション モジュール用 MSI インストーラ ファイル。
anyconnect-gina-win-<*version*>-pre-deploy-k9.msi	SBL オプション モジュール用 MSI インストーラ ファイル。
anyconnect-nam-win-<*version*>.msi	ネットワーク アクセス マネージャ オプション モジュール用 MSI インストーラ ファイル。
anyconnect-posture-win-<*version*>-pre-deploy-k9.msi	ポスチャ オプション モジュール用 MSI インストーラ ファイル。
anyconnect-telemetry-win-<*version*>-pre-deploy-k9.msi	テレメトリ オプション モジュール用 MSI インストーラ ファイル。
anyconnect-websecurity-win-<*version*>-pre-deploy-k9.msi	Web セキュリティ オプション モジュール用 MSI インストーラ ファイル。
anyconnect-win-<*version*>-pre-deploy-k9.msi	AnyConnect コア クライアント用 MSI インストーラ ファイル。
autorun.inf	setup.exe 用セットアップ情報ファイル。
cues_bg.jpg	インストール ユーティリティ GUI の背景画像。
setup.hta	インストール ユーティリティの HTML アプリケーション（HTA）。このプログラムはカスタマイズできます。
update.txt	AnyConnect バージョン番号をリストしたテキスト ファイル。

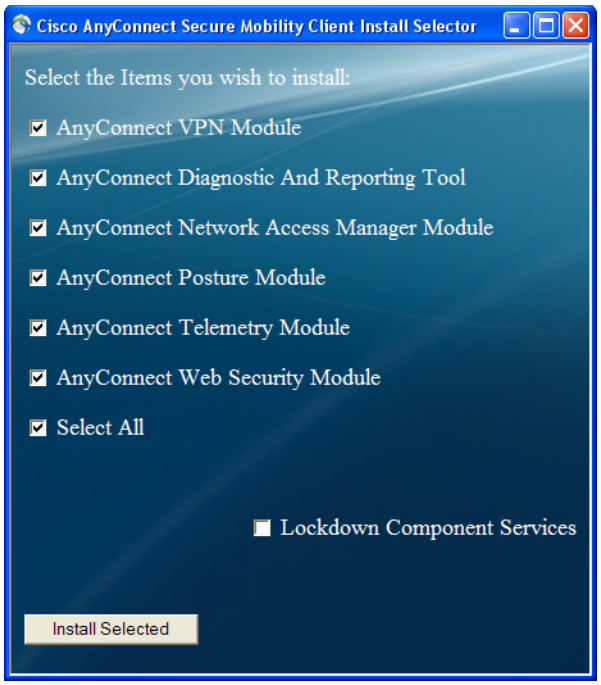
インストール ユーティリティのユーザへの展開

ユーザは、インストール ユーティリティを使用して、インストールする項目を選択します。デフォルトでは、すべてのコンポーネントのチェックボックスがオンです。そのままでよい場合、ユーザは [インストール（Install）] ボタンをクリックして、[Selections To Install] ダイアログボックスにリストされたコンポーネントに同意できます。選択に基づいて、インストールするコンポーネントが判別されます。

インストール ユーティリティは、ISO パッケージ ファイルとしてパッケージ化されている、*setup.hta* という HTML アプリケーション（HTA）です。このプログラムに対しては、任意の変更を、任意に加えることができます。このユーティリティは、必要に応じてカスタマイズしてください。

図 2-18 に、インストール ユーティリティ GUI を示します。

図 2-18　インストール ユーティリティの GUI



各インストーラは、サイレント実行されます。コンピュータのリブートを必要とするインストーラの場合は、インストーラの最終実行後にユーザに通知されます。インストール ユーティリティは、リブートを開始しません。ユーザは、コンピュータを手動でリブートする必要があります。

Windows 用 AnyConnect モジュールで必要とされるインストールまたはアンインストール順序

必要に応じて、ISO イメージから個々のインストーラを取り出して、手動で配布することもできます。事前展開パッケージ内の各インストーラは、個別に実行できます。.iso ファイル内のファイルの表示および解凍には、圧縮ファイル ユーティリティを使用します。

ファイルを手動で配布する場合は、選択したコンポーネント間の依存関係に対処する必要があります。コア クライアント MSI は、オプション モジュールで使用する必要のある、すべての VPN 機能コンポーネントおよび共通コンポーネントを含みます。さらに、オプション モジュール用のインストーラは、前提条件として、同じバージョンの AnyConnect 3.0 コア クライアントがインストールされていることを必要としています。これらのインストーラでは、同じバージョンのコア クライアントが存在していることを確認してから、インストールを始めます。

インストール順序

インストールの順序は重要です。AnyConnect モジュールは次の順番でインストールします。

1. AnyConnect コア クライアント モジュールをインストールします。このモジュールは、GUI および VPN 機能（SSL、IPsec の両方）をインストールします。
2. AnyConnect Diagnostic and Reporting Tool（DART）モジュールをインストール。このモジュールは、AnyConnect コア クライアント インストールに関する、有用な診断情報を提供します。
3. SBL、ネットワーク アクセス マネージャ、Web セキュリティ、ポスチャ モジュールを、任意の順序でインストールします。

4. テレメトリ モジュールをインストールします。このモジュールには、ポスチャ モジュールが必要です。

（注）　オプション モジュール用の個々のインストーラでは、インストールされているコア VPN クライアントのバージョンを確認してから、インストーを行います。 コア モジュールとオプション モジュールのバージョンは一致している必要があります。一致していない場合、オプション モジュールはインストールされず、一致していないことがインストーラからユーザに通知されます。インストール ユーティリティを使用する場合は、パッケージ内のモジュールが、まとめてビルドおよびパッケージ化されるため、バージョンは常に一致します。

アンインストール順序

アンインストールの順序も重要です。次の順序でモジュールをアンインストールします。

1. テレメトリ モジュールをアンインストールします。
2. ネットワーク アクセス マネージャ、Web セキュリティ、ポスチャ、SBL を任意の順序でアンインストールします。
3. AnyConnect コア クライアントをアンインストールします。
4. 最後に DART をアンインストールします。DART 情報は、万一アンインストール プロセスが失敗した場合に役立ちます。

事前展開された AnyConnect モジュールのインストール

AnyConnect モジュールを事前展開する場合、管理者は、事前展開モジュールおよび対応するクライアント プロファイル（モジュールで必要な場合）をエンドポイントにコピーする必要があります。

（注）　ネットワーク アクセス マネージャを使用する場合は、[Hide icon and notifications] オプションを選択して、Windows の事前展開の際に Microsoft の [ネットワーク（Network）] アイコンが表示されないようにする必要があります。デフォルトでは、このアイコンは*通知のみを表示*モードです。このモードでは、変更と更新のアラートが出されます。

以下のモジュールには、AnyConnect クライアント プロファイルが必要です。

- AnyConnect VPN モジュール
- AnyConnect テレメトリ モジュール
- AnyConnect ネットワーク アクセス マネージャ モジュール
- AnyConnect Web セキュリティ モジュール

以下の機能には、AnyConnect クライアント プロファイルは必要ありません。

- AnyConnect VPN Start Before Login
- AnyConnect Diagnostic and Reporting Tool
- AnyConnect ポスチャ モジュール

事前展開モジュールは、「Windows 用 AnyConnect モジュールで必要とされるインストールまたはアンインストール順序」（P.2-31）で説明されている順序でインストールする必要があります。

VPN モジュールとともにオプションの AnyConnect モジュールを事前展開するには、次の手順を実行します。

ステップ 1　**anyconnect-win-<*version*>-pre-deploy-k9.iso** を cisco.com からダウンロードします。

ステップ 2　Winzip、7-zip、または同様のユーティリティを使用して、.iso ファイルの内容を解凍します。

ステップ 3　クライアント プロファイルを必要とするモジュールの場合は、ASDM と統合されているプロファイル エディタかスタンドアロン プロファイル エディタを使用して、インストールするモジュール用のクライアント プロファイルを作成します。さまざまなクライアント プロファイルの設定手順については、次の章を参照してください。

- 第 3 章「VPN アクセスの設定」
- 第 4 章「ネットワーク アクセス マネージャの設定」
- 第 6 章「Web セキュリティの設定」
- 第 7 章「WSA に対する AnyConnect テレメトリの設定」

ステップ 4　作成したクライアント プロファイルは、.iso ファイルから解凍した適切なディレクトリにコピーしてください。

- Profiles\vpn
- Profiles\nam
- Profiles\websecurity
- Profiles\telemetry

ステップ 5　AnyConnect モジュールの事前展開用のパッケージは、表 2-5、「事前展開用 ISO ファイルの内容」で確認してください。

ステップ 6　ソフトウェア管理システムを使用して、事前展開ソフトウェア パッケージと、クライアント プロファイルを含んでいる **Profiles** ディレクトリをエンドポイントに展開します

ステップ 7　「エンタープライズ ソフトウェア展開システム用 MSI ファイルのパッケージ化」（P.2-35）で説明されている手順を実行して、「Windows 用 AnyConnect モジュールで必要とされるインストールまたはアンインストール順序」（P.2-31）に定義されている順序で、AnyConnect モジュールをインストールします。

ネットワーク アクセス マネージャおよび Web セキュリティをスタンドアロン アプリケーションとしてインストールするためのユーザ指示

AnyConnect モジュールのネットワーク アクセス マネージャおよび Web セキュリティは、ユーザ コンピュータ上にスタンドアロン アプリケーションとして展開できます インストール ユーティリティをユーザに展開してある場合は、以下の項目をオンにするようユーザに指示します。

*AnyConnect ネットワーク アクセス マネージャ***および（または）***AnyConnect Web セキュリティ モジュール*

一方、***Cisco AnyConnect VPN モジュール*****はオフにするように指示します。**このようにすると、コア クライアントの VPN 機能がディセーブルになり、ネットワーク アクセス マネージャおよび Web セキュリティが、インストール ユーティリティによって、VPN 機能なしのスタンドアロン アプリケーションとしてインストールされます。

インストール ユーティリティを展開していない場合は、MSI プロパティ PRE_DEPLOY_DISABLE_VPN=1 を設定するようにソフトウェア管理システム（SMS）を設定することにより、VPN 機能をディセーブルにする必要があります。次に、例を示します。

```
msiexec /package anyconnect-win-ver-pre-deploy-k9.msi /norestart /passive
PRE_DEPLOY_DISABLE_VPN=1 /lvx*
```

これを行った場合、MSI では、MSI に埋め込まれた VPNDisable_ServiceProfile.xml ファイルを、VPN 機能のプロファイル用に指定されているディレクトリにコピーします（ファイル パスについては、表 2-15 を参照してください）。

（注） クライアントは、すべての VPN クライアント プロファイルを読み取ります。任意のプロファイルで <ServiceDisable> が true に設定されている場合、VPN は無効になっています。

その後、オプション モジュール用のインストーラを実行できます。このインストーラでは、VPN サービスなしで AnyConnect GUI を使用できます。

ユーザが [Install Selected] ボタンをクリックすると、次の処理が行われます。

ステップ 1　スタンドアロン ネットワーク アクセス マネージャおよびスタンドアロン Web セキュリティ モジュールの選択を確認するポップアップ ダイアログボックスが表示されます。

ステップ 2　ユーザが [OK] をクリックすると、設定値 PRE_DEPLOY_DISABLE_VPN=1 を使用して、インストール ユーティリティにより、AnyConnect 3.0 コア インストーラが起動されます。

ステップ 3　インストール ユーティリティは、既存のすべての VPN プロファイルを削除してから VPNDisable_ServiceProfile.xml をインストールします。

ステップ 4　インストール ユーティリティは、指定に応じて、ネットワーク アクセス マネージャ インストーラおよび Web セキュリティ インストーラを起動します。

ステップ 5　指定に応じて、AnyConnect 3.0 ネットワーク アクセス マネージャおよび Web セキュリティ モジュールが、コンピュータ上で VPN サービスなしでイネーブルになります。

（注） コンピュータ上にネットワーク アクセス マネージャが事前にインストールされていなかった場合、ユーザは、ネットワーク アクセス マネージャのインストールを完了するためにコンピュータをリブートする必要があります。一部のシステム ファイルのアップグレードを必要とする、アップグレード インストールの場合も、ユーザはリブートを必要とします。

エンタープライズ ソフトウェア展開システム用 MSI ファイルのパッケージ化

ここでは、MSI インストール コマンドライン呼び出しなどのエンタープライズ ソフトウェア展開システムを使用して AnyConnect クライアントおよびオプション モジュールを展開するために必要な情報と、プロファイルの展開先の場所について説明します。

- 「MSI インストールのコマンドライン呼び出し」（P.2-35）
- 「AnyConnect プロファイルの展開場所」（P.2-42）
- 「スタンドアロン アプリケーションとしてのネットワーク アクセス マネージャまたは Web セキュリティのインストール」（P.2-36）
- 「AnyConnect をプログラムの追加と削除のリストから非表示にする MSI コマンド」（P.2-36）

MSI インストールのコマンドライン呼び出し

表 2-6 に、個々の AnyConnect モジュールをインストールするために使用する、MSI インストールのコマンドライン呼び出しを示します。コマンドによって生成されるログ ファイルも示してあります。

表 2-6　MSI インストールのコマンドライン呼び出しおよび生成されるログ ファイル

インストールされるモジュール	コマンドおよびログ ファイル
VPN なしの AnyConnect コア クライアント機能。 スタンドアロン ネットワーク アクセス マネージャまたは Web セキュリティ モジュールをインストールするときに使用します。	msiexec /package anyconnect-win-ver-pre-deploy-k9.msi /norestart /passive PRE_DEPLOY_DISABLE_VPN=1 /lvx* anyconnect-win-<*version*>-pre-deploy-k9-install-datetimestamp.log
VPN ありの AnyConnect コア クライアント機能。	msiexec /package anyconnect-win-ver-pre-deploy-k9.msi /norestart /passive /lvx* anyconnect-win-<*version*>-pre-deploy-k9-install-datetimestamp.log
Diagnostic and Reporting Tool（DART）	msiexec /package anyconnect-dart-win-ver-k9.msi /norestart /passive /lvx* anyconnect-dart-<*version*>-pre-deploy-k9-install-datetimestamp.log
SBL	msiexec /package anyconnect-gina-win-ver-k9.msi /norestart /passive /lvx* anyconnect-gina-<*version*>-pre-deploy-k9-install-datetimestamp.log
ネットワーク アクセス マネージャ	msiexec /package anyconnect-nam-win-ver-k9.msi /norestart /passive /lvx* anyconnect-nam-<*version*>-pre-deploy-k9-install-datetimestamp.log
Web セキュリティ	msiexec /package anyconnect-websecurity-win-ver-pre-deploy-k9.msi /norestart/passive /lvx* anyconnect-websecurity-<*version*>-pre-deploy-k9-install-datetimestamp.log
ポスチャ	msiexec /package anyconnect-posture-win-ver-pre-deploy-k9.msi /norestart/passive /lvx* anyconnect-posture-<*version*>-pre-deploy-k9-install-datetimestamp.log
テレメトリ	msiexec /package anyconnect-telemetry-win-ver-pre-deploy-k9.msi /norestart /passive /lvx* anyconnect-telemetry-<*version*>-pre-deploy-k9-install-datetimestamp.log

スタンドアロン アプリケーションとしてのネットワーク アクセス マネージャまたは Web セキュリティのインストール

ネットワーク アクセス マネージャまたは Web セキュリティを VPN サービスなしでインストールするには、次のコマンドを実行する必要があります。

```
msiexec /package anyconnect-win-ver-pre-deloy-k9.msi /norestart /passive
PRE_DEPLOY_DISABLE_VPN=1
```

コア クライアント用の MSI を実行すると、コア クライアントがインストールまたは更新され、既存のすべてのプロファイルが削除されて、プロファイルの場所に VPNDisable_ServiceProfile.xml がインストールされます。その後、オプション モジュール用のインストーラを実行できます。その後、スタンドアロン コンポーネントでは、VPN サービスなしで AnyConnect GUI を使用できます。

AnyConnect をプログラムの追加と削除のリストから非表示にする MSI コマンド

Windows のプログラムの追加と削除リストを表示するユーザに対して、インストールされている AnyConnect モジュールを非表示にできます。ARPSYSTEMCOMPONENT=1 を使用して任意のインストーラを起動した場合、そのモジュールは、Windows のプログラムの追加と削除リストに表示されません。

本書に記載されているトランスフォームの例を使用して、非表示にするモジュールごとの各 MSI インストーラにトランスフォームを適用しながら、このプロパティを設定することをお勧めします。

レガシー クライアントおよびオプション モジュールのアップグレード

前のバージョンをアップグレードする場合、AnyConnect Secure Mobility Client バージョン 3.0 は、以下の処理を行います。

- 前のバージョンの全コア クライアントをアップグレードし、すべての VPN 設定を保持します。
- Cisco SSC 5.x をネットワーク アクセス マネージャ モジュールにアップグレードし、ネットワーク アクセス マネージャで使用するためにすべての SSC 設定を保持し、SSC 5.x を削除します。
- Cisco セキュア デスクトップで使用するホスト スキャン ファイルをアップグレードします。AnyConnect 3.0 クライアントは、セキュア デスクトップと共存できます。
- Cisco IPsec VPN クライアントはアップグレード***しません***（削除もしません）。ただし、AnyConnect 3.0 クライアントは、コンピュータ上で IPsec VPN クライアントと共存できます。
- ScanSafe Web セキュリティ機能は、アップグレード***せず***、同じコンピュータ上で共存できません。AnyWhere+ をアンインストールする必要があります。

インストーラのカスタマイズとローカライズ

トランスフォームを使用して Windows 用 AnyConnect コア インストーラをカスタマイズでき、コア インストーラの表示するメッセージを、リモート ユーザの優先言語に翻訳できます。AnyConnect のクライアントとインストーラのカスタマイズとローカライズ（翻訳）の詳細については、第 11 章「AnyConnect クライアントとインストーラのカスタマイズとローカライズ」を参照してください。

Linux および Mac OS X コンピュータへの事前展開

以下の項では、Linux および Mac OS X コンピュータへの事前展開に特化した情報を示します。内容は次のとおりです。

- 「Linux および MAC OS X 用モジュールの場合の推奨されるインストールまたはアンインストールの順序」（P.2-37）

Linux および MAC OS X 用モジュールの場合の推奨されるインストールまたはアンインストールの順序

Linux および Mac 用の個々のインストーラを取り出して、手動で配布できます。事前展開パッケージ内の各インストーラは、個別に実行できます。tar.gz ファイルまたは .dmg ファイル内のファイルの表示および解凍には、圧縮ファイル ユーティリティを使用します。

ファイルを手動で配布する場合は、次のインストール順序を強くお勧めします。

1. AnyConnect コア クライアント モジュールをインストールします。このモジュールは、GUI および VPN 機能（SSL、IPsec の両方）をインストールします。
2. DART モジュールをインストールします。このモジュールは、AnyConnect コア クライアント インストールに関する、有用な診断情報を提供します。
3. ポスチャ モジュールをインストールします。

AnyConnect モジュールのアンインストール

アンインストールの順序も重要です。次の順序でモジュールをアンインストールします。

1. ポスチャ モジュールをアンインストールします。
2. AnyConnect コア クライアントをアンインストールします。
3. 最後に DART をアンインストールします。DART 情報は、万一アンインストール プロセスが失敗した場合に役立ちます。

Ubuntu 9.x 64 ビットを実行しているコンピュータの場合の AnyConnect 要件

Ubuntu 9.x 64 ビットを実行しているコンピュータ上で Cisco AnyConnect Secure Mobility Client を実行するために、AnyConnect では、以下の要件を必要とします。

- 32 ビット互換ライブラリがコンピュータ上にインストールされている。
- Ubuntu 9.x 32 ビット バージョンの NSS 暗号ライブラリが /usr/local/firefox にインストールされている。
- Firefox 証明書ストアと対話できるようにユーザ ホーム ディレクトリに格納された .mozilla/firefox プロファイル

これらの問題に対処するには、次の手順を実行します。

ステップ 1　次のコマンドを入力して、32 ビット互換ライブラリをインストールします。

```
administrator@ubuntu-904-64:/usr/local$ sudo apt-get install ia32-libs lib32nss-mdns
```

ステップ 2　32 ビット版の FireFox を http://www.mozilla.com からダウンロードして、/usr/local/firefox にインストールします。

AnyConnect は、必要な NSS 暗号化ライブラリを先にこのディレクトリで検索します。

ステップ 3　次のコマンドを入力して、ここで示すディレクトリに Firefox インストールを展開します。

```
administrator@ubuntu-904-64:/usr/local$ sudo tar -C /usr/local -xvjf
~/Desktop/firefox-version.tar.bz2
```

ステップ 4　AnyConnect を使用するユーザとしてログインし、少なくとも 1 回、Firefox を実行します。

これによって、AnyConnect が Firefox 証明書ストアと対話するために必要な .mozilla/firefox プロファイルがユーザのホーム ディレクトリに作成されます。

ステップ 5　Standalone モードで AnyConnect をインストールします。

Mac OS X で Java インストーラが失敗した場合の手動インストール オプションの使用

Mac 上で WebLaunch を使用して AnyConnect を起動し、Java インストーラが失敗した場合は、ダイアログボックスに [手動インストール（Manual Install）] リンクが表示されます。この場合、ユーザは、次の手順を実行する必要があります。

ステップ 1　[手動インストール（Manual Install）] をクリックします。ダイアログボックスに、vpnsetup.sh ファイルを保存するオプションが表示されます。

ステップ 2　vpnsetup.sh ファイルを Mac 上に保存します。

ステップ 3　ターミナル ウィンドウを開き、CD コマンドを使用して、保存したファイルがあるディレクトリに移動します。

ステップ 4　次のコマンドを入力します。

```
sudo /bin/sh vpnsetup.sh
```

vpnsetup スクリプトによって AnyConnect インストールが開始されます。

ステップ 5　インストール後、[アプリケーション（Applications）] > [Cisco] > [Cisco AnyConnect Secure Mobility Client] の順に選択して、AnyConnect セッションを開始します。

システムでのアプリケーションの制限

Mac OS X 10.8 では、システムで動作できるアプリケーションを制限するゲートキーパーという新機能が導入されています。次からダウンロードされたアプリケーションを許可するか選択できます。

- Mac App Store
- Mac App Store and identified developers
- あらゆる場所

デフォルト設定は **Mac App Store and identified developers**（署名付きアプリケーション）です。AnyConnect は、署名付きのアプリケーションで、この設定または **Anywhere** 設定で通常実行されます。**Mac App Store** 設定を選択した場合、AnyConnect をインストールおよび実行するには、Ctrl キーを押しながらクリックする必要があります。詳細については、http://www.apple.com/macosx/mountain-lion/security.html を参照してください。

（注）　これは新しいスタンドアロンのインストールにのみ適用され、Web の起動または OS のアップグレード（たとえば、10.7 から 10.8）には適用されません。

Firefox によるサーバ証明書の検証

AnyConnect を Linux デバイスにインストールした後、AnyConnect 接続を初めて試行する前に、Firefox ブラウザを開始します。AnyConnect では、Firefox を使用してサーバ証明書を検証します。Firefox を開くとプロファイルが作成されます。このプロファイルなしでは、サーバ証明書を信頼済みであると検証できません。

Firefox を使用しない場合は、Firefox 証明書ストアを除外するようにローカル ポリシーを設定する必要があります。これには、PEM ストアの設定も必要です。

AnyConnect ファイル情報

ここでは、次の項で、ユーザ コンピュータ上の AnyConnect ファイルの場所について説明します。

- 「エンドポイント コンピュータ上のモジュールのファイル名」（P.2-39）
- 「ローカル コンピュータにインストールされたユーザ プリファレンス」（P.2-43）
- 「AnyConnect プロファイルの展開場所」（P.2-42）

エンドポイント コンピュータ上のモジュールのファイル名

表 2-7 に、クライアントを事前展開または ASA 展開するときのエンドポイント コンピュータ上の AnyConnect ファイル名を、オペレーティング システム タイプごとに示します。

表 2-7　ASA 展開または事前展開用の AnyConnect コア ファイル名

AnyConnect 3.0 コア	Web-Deploy インストーラ（ダウンロード）	事前展開インストーラ
Windows	anyconnect-win-(ver)-web-deploy-k9.exe	anyconnect-win-(ver)-pre-deploy-k9.msi
Mac	anyconnectsetup.dmg	anyconnect-macosx-i386-(ver)-k9.dmg
Linux	anyconnectsetup.sh	anyconnect-linux-(ver)-k9.tar.gz

表 2-8 に、クライアントを事前展開または ASA 展開するときのエンドポイント コンピュータ上の DART ファイル名を、オペレーティング システム タイプごとに示します。3.0.3050 よりも前のリリースでは、DART コンポーネントは Web 展開用に個別のダウンロード（dmg、.sh、または .msi ファイル）になっていました。リリース 3.0.3050 以降では、DART コンポーネントは .pkg ファイルに含まれています。

表 2-8　ASA 展開または事前展開用の DART パッケージ ファイル名

DART	Web-Deploy ファイル名およびパッケージ（ダウンロード）	Pre-Deploy インストーラ
Windows	*リリース 3.0.3050 以降：* anyconnect-win-(ver)-k9.pkg	anyconnect-win-(ver)-pre-deploy-k9.iso
	3.0.3050 よりも前のリリース： anyconnect-dart-win-(ver)-k9.msi*	anyconnect-dart-win-(ver)-k9.msi*
Mac	*リリース 3.0.3050 以降：* anyconnect-macosx-i386-(ver)-k9.pkg	anyconnect-macosx-i386-(ver)-k9.dmg
	3.0.3.050 よりも前のリリース： anyconnect-dartsetup.dmg	anyconnect-dart-macosx-i386-(ver)-k9.dmg
Linux	*リリース 3.0.3050 以降：* anyconnect-linux-(ver)-k9.pkg	anyconnect-predeploy-linux-(ver)-k9.tar.gz
	3.0.3050 よりも前のリリース： anyconnect-dartsetup.sh	anyconnect-dart-linux-(ver)-k9.tar.gz

* Web 展開パッケージおよび事前展開パッケージは、ISO イメージ（*.iso）に含まれています。ISO イメージ ファイルには、ユーザのコンピュータへの展開に必要なプログラムと MSI インストーラ ファイルが含まれています。

表 2-9 に、クライアントを Windows コンピュータに事前展開または ASA 展開するときの、エンドポイント コンピュータ上の SBL ファイル名を示します。

表 2-9　ASA 展開または事前展開用の Start Before Logon パッケージ ファイル名

SBL (Gina)	Web-Deploy インストーラ（ダウンロード）	Pre-Deploy インストーラ
Windows	anyconnect-gina-win-(ver)-web-deploy-k9.exe	anyconnect-gina-win-(ver)-pre-deploy-k9.msi

表 2-10 に、クライアントを Windows コンピュータに事前展開または ASA 展開するときの、エンドポイント コンピュータ上のネットワーク アクセス マネージャ ファイル名を示します。

表 2-10　ASA 展開または事前展開用のネットワーク アクセス マネージャ ファイル名

Network Access Manager	Web-Deploy インストーラ（ダウンロード）	Pre-Deploy インストーラ
Windows	anyconnect-nam-win-(ver)-k9.msi	anyconnect-nam-win-(ver)-k9.msi

表 2-11 に、クライアントを事前展開または ASA 展開するときのエンドポイント コンピュータ上のポスチャ モジュール ファイル名を、オペレーティング システム タイプごとに示します。

表 2-11　ASA 展開または事前展開用のポスチャ モジュール ファイル名

Posture	Web-Deploy インストーラ（ダウンロード）	Pre-Deploy インストーラ
Windows	anyconnect-posture-win-(ver)-web-deploy-k9.msi	anyconnect-posture-win-(ver)-pre-deploy-k9.msi
Mac	anyconnect-posturesetup.dmg	anyconnect-posture-macosx-i386-(ver)-k9.dmg
Linux	anyconnect-posturesetup.sh	anyconnect-posture-linux-(ver)-k9.tar.gz

表 2-12 に、クライアントを事前展開または ASA 展開するときのエンドポイント コンピュータ上の Windows 用テレメトリ モジュールのファイル名を示します。

表 2-12　ASA 展開または事前展開用のテレメトリ ファイル名

Telemetry	Web-Deploy インストーラ（ダウンロード）	Pre-Deploy インストーラ
Windows	anyconnect-telemetry-win-(ver)-web-deploy-k9.exe. Dependent upon installation of anyconnect-posture-win-(ver)-web-deploy-k9.msi	anyconnect-telemetry-win-(ver)-pre-deploy-k9.msi. Dependent upon installation of anyconnect-posture-win-(ver)-pre-deploy-k9.msi.

表 2-13 に、クライアントを事前展開または ASA 展開するときのエンドポイント コンピュータ上の Windows 用 Web セキュリティ モジュールのファイル名を示します。

表 2-13　ASA 展開または事前展開用の Web セキュリティ ファイル名

Web Security	Web-Deploy インストーラ（ダウンロード）	事前展開インストーラ
Windows	anyconnect-websecurity-win-(ver)-web-deploy-k9.exe	anyconnect-websecurity-win-(ver)-pre-deploy-k9.msi

AnyConnect プロファイルの展開場所

表 2-14 に、AnyConnect によってローカル コンピュータにダウンロードされるプロファイル関連のファイルおよびファイルの目的を示します。

表 2-14　エンドポイント上のプロファイル ファイル

ファイル	説明
anyfilename.xml	AnyConnect プロファイル。このファイルは、特定のユーザ タイプに対して設定される機能および属性値を指定します。
AnyConnectProfile.tmpl	AnyConnect ソフトウェアに付属するクライアント プロファイルの例。
AnyConnectProfile.xsd	XML スキーマ フォーマットを定義します。AnyConnect はこのファイルを使用して、プロファイルを確認します。

表 2-15 に、すべてのオペレーティング システムについて、AnyConnect プロファイルの場所を示します。

表 2-15　すべてのオペレーティング システムに対するプロファイルの場所

オペレーティング システム	モジュール	ロケーション
Windows XP	VPN を使用するコア クライアント	%ALLUSERSPROFILE%\Application Data\Cisco\ Cisco AnyConnect Secure Mobility Client\Profile
	ネットワーク アクセス マネージャ	%ALLUSERSPROFILE%\Application Data\Cisco\ Cisco AnyConnect Secure Mobility Client\NetworkAccessManager\newConfigFiles
	テレメトリ	%ALLUSERSPROFILE%\Application Data\Cisco\ Cisco AnyConnect Secure Mobility Client\Telemetry
	Web セキュリティ	%ALLUSERSPROFILE%\Application Data\Cisco\ Cisco AnyConnect Secure Mobility Client\Web Security
Windows Vista	VPN を使用するコア クライアント	%ProgramData%\Cisco\Cisco AnyConnect Secure Mobility Client\Profile
	ネットワーク アクセス マネージャ	%ProgramData%\Cisco\ Cisco AnyConnect Secure Mobility Client\NetworkAccessManager\newConfigFiles
	テレメトリ	%ProgramData%\Cisco\ Cisco AnyConnect Secure Mobility Client\Telemetry
	Web セキュリティ	%ProgramData%\Cisco\ Cisco AnyConnect Secure Mobility Client\Web Security

表 2-15　すべてのオペレーティング システムに対するプロファイルの場所

オペレーティング システム	モジュール	ロケーション
Windows 7	VPN を使用するコア クライアント	%ProgramData%\Cisco\Cisco AnyConnect Secure Mobility Client\Profile
	ネットワーク アクセス マネージャ	%ProgramData%\Cisco\ Cisco AnyConnect Secure Mobility Client\NetworkAccessManager\newConfigFiles
	テレメトリ	%ProgramData%\Cisco\ Cisco AnyConnect Secure Mobility Client\Telemetry
	Web セキュリティ	%ProgramData%\Cisco\ Cisco AnyConnect Secure Mobility Client\Web Security
Mac OS X	すべてのモジュール	/opt/cisco/anyconnect/profile
Linux	すべてのモジュール	/opt/cisco/anyconnect/profile

ローカル コンピュータにインストールされたユーザ プリファレンス

また一部のプロファイル設定は、ユーザ コンピュータ上のユーザ プリファレンス ファイルまたはグローバル プリファレンス ファイルにローカルに保存されます。ユーザ ファイルには、クライアント GUI の [プリファレンス（Preferences）] タブにユーザ制御可能設定をクライアントで表示するうえで必要となる情報、およびユーザ、グループ、ホストなど、直近の接続に関する情報が保存されます。

グローバル ファイルには、ユーザ制御可能設定に関する情報が保存されます。これにより、ログイン前でも（ユーザがいなくても）それらの設定を適用することができます。たとえば、クライアントでは Start Before Logon や起動時自動接続が有効になっているかどうかをログイン前に認識する必要があります。

表 2-16 に、クライアント コンピュータ上のプリファレンス ファイルのファイル名およびインストール先パスを示します。

表 2-16　ユーザ プリファレンス ファイルおよびインストール パス

オペレーティング システム	タイプ	ファイルおよびパス
Windows Vista Windows 7	ユーザ	C:\Users*username*\AppData\Local\Cisco\ Cisco AnyConnect Secure Mobility Client\preferences.xml
	グローバル	C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\ preferences_global.xml
Windows XP	ユーザ	C:\Documents and Settings**username**\Local Settings\ApplicationData\ Cisco\Cisco AnyConnect Secure Mobility Client\preferences.xml
	グローバル	C:\Documents and Settings\AllUsers\Application Data\Cisco\ Cisco AnyConnect Secure Mobility Client\preferences_global.xml
Mac OS X	ユーザ	/Users/username/.anyconnect
	グローバル	/opt/cisco/anyconnect/.anyconnect_global

オペレーティング システム	タイプ	ファイルおよびパス
Linux	ユーザ	/home/username/.anyconnect
	グローバル	/opt/cisco/anyconnect/.anyconnect_global

スタンドアロン AnyConnect プロファイル エディタの使用

スタンドアロン AnyConnect プロファイル エディタを使用すると、管理者は、VPN 用、ネットワーク アクセス マネージャ用、AnyConnect Secure Mobility Client のための Web セキュリティ モジュール用のクライアント プロファイルを設定できます。これらのプロファイルは、VPN 用、ネットワーク アクセス マネージャ用、Web セキュリティ モジュール用の事前展開キットを使用して配布できます。

スタンドアロン プロファイル エディタのシステム要件

サポートされるオペレーティング システム

このアプリケーションは、Windows XP 上と Windows 7 上でテストされています。MSI は、Windows 上だけで実行されます。

Java 要件

このアプリケーションは、JRE 1.6 を必要とします。インストールされていない場合は、MSI インストーラによって自動的にインストールされます。

ブラウザ要件

このアプリケーションに含まれているヘルプ ファイルは、Firefox および Internet Explorer でサポートされています。その他のブラウザではテストされていません。

必要なハード ドライブ容量

Cisco AnyConnect プロファイル エディタ アプリケーションは、最大 5 MB のハード ドライブ容量を必要とします。JRE 1.6 は、最大 100 MB のハード ドライブ容量を必要とします。

スタンドアロン AnyConnect プロファイル エディタのインストール

スタンドアロン AnyConnect プロファイル エディタは、AnyConnect の ISO ファイルおよび .pkg ファイルとは別に Windows 実行ファイル（.exe）として配布され、ファイルの命名規則は **anyconnect-profileeditor-win-**<*version*>**-k9.exe** となっています。

スタンドアロン プロファイル エディタをインストールするには、次の手順を実行します。

ステップ 1　Cisco.com から **anyconnect-profileeditor-win-**<*version*>**-k9.exe** をダウンロードします。

ステップ 2　**anyconnect-profileeditor-win-**<*version*>**-k9.exe** をダブルクリックして、インストール ウィザードを起動します。

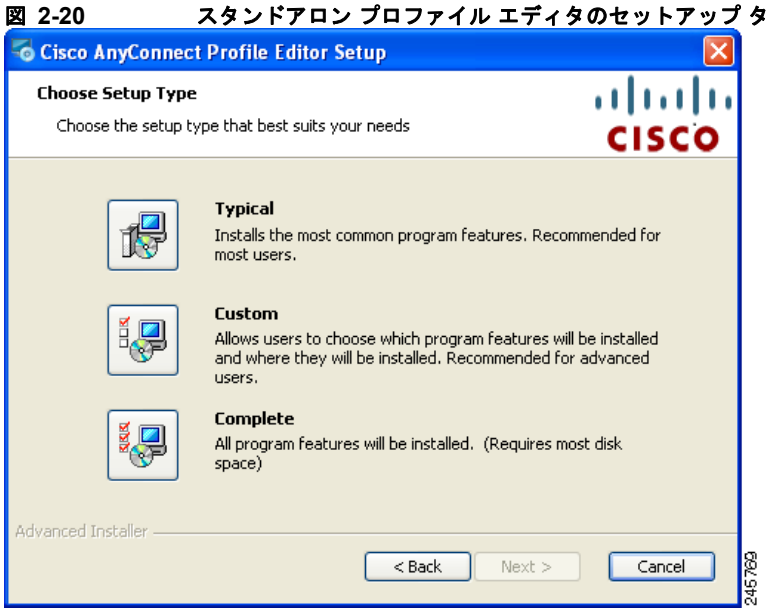
ステップ 3　[ようこそ（Welcome）] 画面で、[次へ（Next）] をクリックします。

図 2-19　スタンドアロン プロファイル エディタの [ようこそ（Welcome）] 画面

ステップ 4　[セットアップ タイプの選択（Choose Setup Type）] ウィンドウで、次のいずれかのボタンをクリックし、[次へ（Next）] をクリックします。

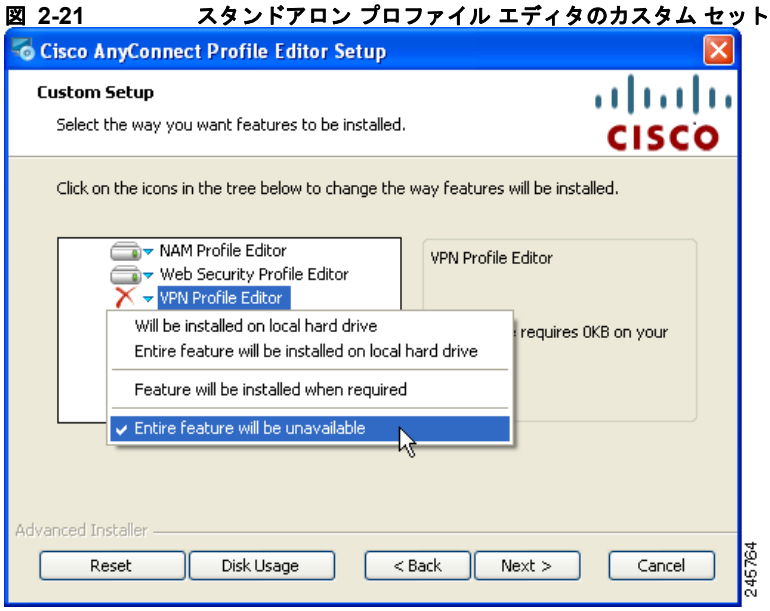
- [標準（Typical）]：ネットワーク アクセス マネージャ プロファイル エディタのみが自動的にインストールされます。
- [カスタム（Custom）]：ネットワーク アクセス マネージャ プロファイル エディタ、Web セキュリティ プロファイル エディタ、VPN プロファイル エディタから任意のプロファイル エディタを選択してインストールできます。
- [フル（Complete）]：ネットワーク アクセス マネージャ プロファイル エディタ、Web セキュリティ プロファイル エディタ、VPN プロファイル エディタが自動的にインストールされます。

図 2-20　スタンドアロン プロファイル エディタのセットアップ タイプの選択



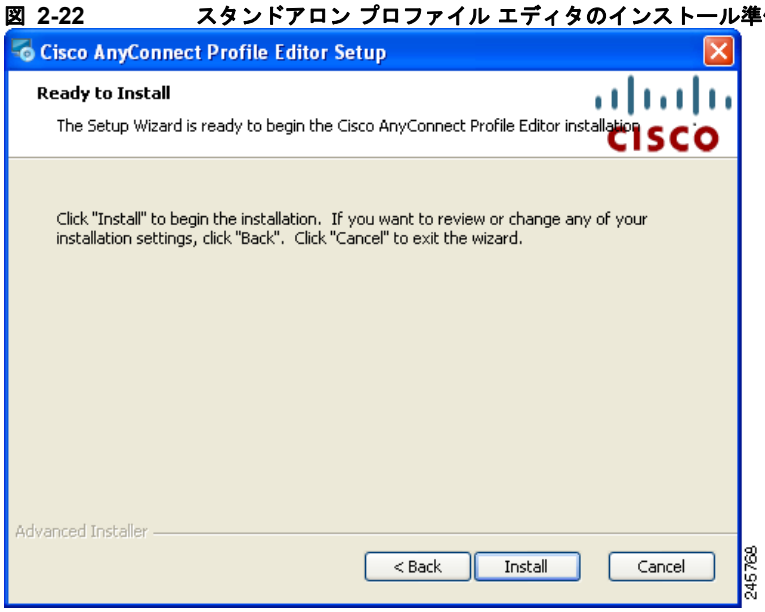
ステップ 5　前のステップで [標準（Typical）] または [フル（Complete）] をクリックした場合は、ステップ 6 までスキップしてください。前のステップで [カスタム（Custom）] をクリックした場合は、インストールするスタンドアロン プロファイル エディタのアイコンをクリックし、[ローカルのハード ドライブにインストールする（Will be installed on local hard drive）] を選択するか、[すべての機能を利用しない（Entire Feature will be unavailable）] をクリックして、そのスタンドアロン プロファイル エディタがインストールされないようにします。[次へ（Next）] をクリックします。

図 2-21　スタンドアロン プロファイル エディタのカスタム セットアップ



ステップ 6　[インストール準備完了（Ready to Install）] 画面で [インストール（Install）] をクリックします。[Cisco AnyConnect プロファイル エディタのインストール（Installing Cisco AnyConnect Profile Editor）] 画面にインストールの進行状況が表示されます。

図 2-22　スタンドアロン プロファイル エディタのインストール準備完了



ステップ 7　[Cisco AnyConnect プロファイル エディタ セットアップ ウィザードの完了（Completing the Cisco AnyConnect Profile Editor Setup Wizard）] で [完了（Finish）] をクリックします。

図 2-23　スタンドアロン プロファイル エディタのインストールが完了

- スタンドアロン AnyConnect プロファイル エディタは、**C:\Program Files\Cisco\Cisco AnyConnect Profile Editor** ディレクトリにインストールされます。
- [スタート（Start）] > [すべてのプログラム（All Programs）] > [Cisco] > [Cisco AnyConnect Profile Editor] を選択してから、サブメニューで目的のスタンドアロン プロファイル エディタをクリックするか、デスクトップ上にインストールされる該当するプロファイル エディタ ショートカット アイコンをクリックすることにより、VPN、ネットワーク アクセス マネージャ、Web セキュリティのプロファイル エディタを起動できます。

スタンドアロン AnyConnect プロファイル エディタ インストールの修正

次の手順を実行することにより、VPN、ネットワーク アクセス マネージャ、または Web セキュリティのプロファイル エディタをインストールまたは削除するように、スタンドアロン Cisco AnyConnect プロファイル エディタ インストールを修正できます。

ステップ 1　Windows のコントロール パネルを開いて [プログラムの追加または削除（Add or Remove Programs）] をクリックします。

ステップ 2　[Cisco AnyConnect Profile Editor] を選択し、[変更（Change）] をクリックします。

ステップ 3　[次へ（Next）] をクリックします。

ステップ 4　[変更（Modify）] をクリックします。

ステップ 5　インストールまたは削除するプロファイル エディタのリストを編集し、[次へ（Next）] をクリックします。

ステップ 6　[インストール（Install）] をクリックします。

ステップ 7　[完了（Finish）] をクリックします。

スタンドアロン AnyConnect プロファイル エディタのアンインストール

ステップ 1　Windows のコントロール パネルを開いて [プログラムの追加または削除（Add or Remove Programs）] をクリックします。

ステップ 2　Cisco AnyConnect プロファイル エディタを選択し、[削除（Remove）] をクリックします。

ステップ 3　[はい（Yes）] をクリックして、Cisco AnyConnect プロファイル エディタをアンインストールすることを確認します。

（注）　スタンドアロン プロファイル エディタをアンインストールするときに、JRE 1.6 は自動的にアンインストールされません。別途アンインストールする必要があります。

スタンドアロン プロファイル エディタを使用したクライアント プロファイルの作成

ステップ 1　VPN、ネットワーク アクセス マネージャ、または Web セキュリティのプロファイル エディタを起動します。これには、デスクトップ上のアイコンをダブルクリックするか、[スタート（Start）] > [すべてのプログラム（All Programs）] > [Cisco] > [Cisco AnyConnect Profile Editor] の順に選択してサブメニューから VPN、ネットワーク アクセス マネージャ、または Web セキュリティのプロファイル エディタを選択します。

ステップ 2　『AnyConnect Administrator Guide』の以下の章にある、クライアント プロファイルの作成手順を実行します。

- 第 3 章「VPN アクセスの設定」

- 第 4 章「ネットワーク アクセス マネージャの設定」
- 第 6 章「Web セキュリティの設定」

ステップ 3　[ファイル（File）] > [保存（Save）] を選択して、クライアント プロファイルを保存します。プロファイル エディタの各パネルには、クライアント プロファイルのパスおよびファイル名が表示されます。

スタンドアロン プロファイル エディタを使用したクライアント プロファイルの編集

ステップ 1　VPN、ネットワーク アクセス マネージャ、または Web セキュリティのプロファイル エディタを起動します。これには、デスクトップ上のアイコンをダブルクリックするか、[スタート（Start）] > [すべてのプログラム（All Programs）] > [Cisco] > [Cisco AnyConnect Profile Editor] の順に選択してサブメニューから VPN、ネットワーク アクセス マネージャ、または Web セキュリティのプロファイル エディタを選択します。

ステップ 2　[ファイル（File）] > [オープン（Open）] を選択し、編集するクライアント プロファイル XML ファイルまで移動します。

（注）　たとえば、Web セキュリティ機能のクライアント プロファイルを、誤って、VPN など別の機能のプロファイル エディタを使用して開こうとすると、「Schema Validation failed」というメッセージが表示され、プロファイルを編集できません。

ステップ 3　プロファイルに変更を加え、[ファイル（File）] > [保存（Save）] を選択して変更を保存します。

（注）　誤って、同じ種類のプロファイル エディタのインスタンスを 2 つ使用して、同じクライアント プロファイルを編集しようとした場合は、そのクライアント プロファイルに加えた最後の変更が保存されます。

AnyConnect Secure Mobility ソリューションの WSA をサポートするための ASA の設定

現在、ユーザとその所有デバイスは、オフィス、自宅、空港、カフェといったさまざまな場所からインターネットに接続するなど、さらにモバイル化が進んでいます。従来、ネットワーク内のユーザはセキュリティの脅威から保護されていましたが、従来のネットワーク外のユーザはアクセプタブル ユース ポリシーが適用されずにマルウェアから最小限しか保護されないため、現在よりもデータ損失のリスクが高まっています。

雇用主は、従業員やパートナーが場所やデバイスを問わずに作業できるフレキシブルな作業環境の創出を望んでいますが、同時に、企業の利益と資産をインターネット ベースの脅威から常時保護したいと考えています。

従来のネットワーク セキュリティ ソリューションやコンテンツ セキュリティ ソリューションは、ユーザと資産をネットワーク ファイアウォールで保護する点では理想的でしたが、ユーザまたはデバイスがネットワークに接続していない場合や、セキュリティ ソリューションを介してデータがルーティングされない場合には効果がありません。

シスコは AnyConnect Secure Mobility を提供してリモート エンドポイントへのネットワーク境界を拡張し、Web セキュリティ アプライアンスで提供される Web フィルタリング サービスをシームレスに統合できます。Cisco AnyConnect Secure Mobility は、コンピュータ対応プラットフォームやスマートフォン対応プラットフォーム上のモバイル ユーザを保護する革新的な新しい方法を実現し、エンドユーザには、よりシームレスな常時保護されたエクスペリエンスが提供され、IT 管理者は包括的にポリシーを適用できるようになります。

AnyConnect Secure Mobility は、次のシスコ製品全体の機能のコレクションです。

- Cisco IronPort Web セキュリティ アプライアンス（WSA）
- Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンス（ASA）
- Cisco AnyConnect クライアント

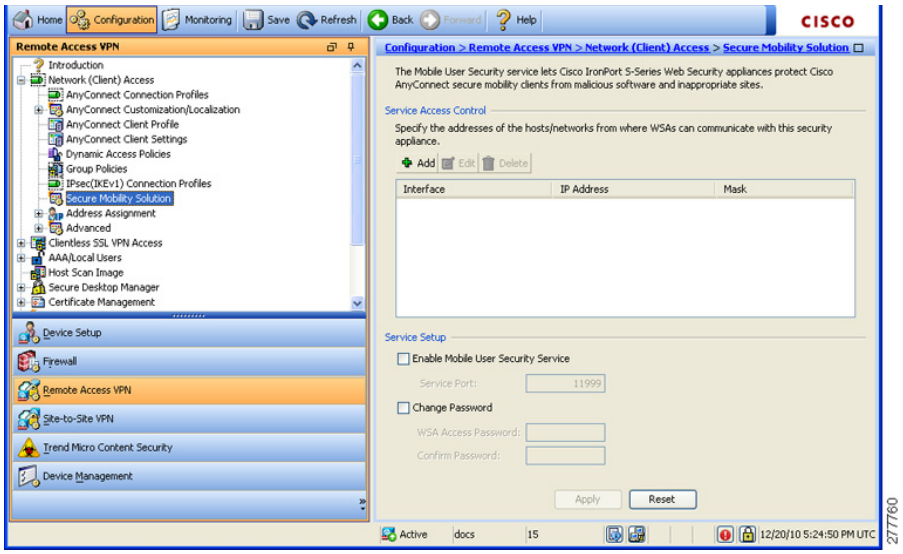
Cisco AnyConnect Secure Mobility は、次の機能を提供してモバイル ワークフォースの課題に対処します。

- **セキュアかつ持続的な接続**：（適応型セキュリティ アプライアンスをヘッドエンドに使用する）Cisco AnyConnect は、AnyConnect Secure Mobility のリモート アクセス接続機能部分を提供します。ネットワークへのアクセスを許可する前に、ユーザとデバイスの両方を認証して検証する必要があるため、セキュアな接続が得られます。通常、Cisco AnyConnect はネットワーク間のローミング時も常時接続に設定されるため、接続は固定されます。Cisco AnyConnect は常時接続でありながら、十分な柔軟性も備えているため、ロケーションに応じてさまざまなポリシーを適用できます。また、インターネットにアクセスする前に契約条項に同意する必要がある「キャプティブ ポータル」で、ユーザのインターネット アクセスを許可します。
- **持続的なセキュリティとポリシーの適用**：Web セキュリティ アプライアンスは、アクセプタブル ユース ポリシーやマルウェアからの保護などのコンテキストに対応したポリシーを、モバイル（リモート）ユーザも含めたあらゆるユーザに適用します。また Web セキュリティ アプライアンスは、AnyConnect クライアントからユーザ認証情報を受け入れ、ユーザが Web コンテンツにアクセスできるよう自動認証手順を提供します。

[セキュア モビリティ ソリューション（Secure Mobility Solution）] ダイアログ ボックスを使用して、この機能の ASA 部分を設定します。AnyConnect Secure Mobility により Cisco IronPort S シリーズ Web セキュリティ アプライアンスは Cisco AnyConnect セキュア モビリティ クライアントをスキャンでき、クライアントを悪意あるソフトウェアや不適切なサイトから確実に保護します。クライアントは、Cisco IronPort S シリーズ Web セキュリティ アプライアンス保護がイネーブルになっているか定期的に確認します。

WSA サポートのために ASA を設定するには、ASDM を起動し、[設定（Configuration）] > [リモート アクセス VPN（Remote Access VPN）] > [ネットワーク（クライアント）アクセス（Network (Client) Access）] > [セキュア モビリティ ソリューション（Secure Mobility Solution）] パネルを選択します（図 2-24 を参照）。詳細については [ヘルプ（Help）] をクリックします。

図 2-24　AnyConnect Secure Mobility ウィンドウ



（注）

- この機能では、Cisco AnyConnect セキュア モビリティ クライアントの AnyConnect Secure Mobility ライセンスをサポートする Cisco IronPort Web セキュリティ アプライアンスのリリースが必要です。また、AnyConnect Secure Mobility 機能をサポートする AnyConnect リリースが必要です。
- この機能は、SSL プロトコルまたは IPsec IKEv2 プロトコルを使用した AnyConnect 接続で使用可能です。

ステップ 1　次のいずれかの方法を使用して、どのホストまたはネットワーク アドレスから WSA が通信し、リモート ユーザを識別できるかを指定します。

- **IP アドレスによる関連付け**：Web セキュリティ アプライアンス管理者は、リモート デバイスに割り当てられていると見なす IP アドレスの範囲を指定します。通常、適応型セキュリティ アプライアンスは、VPN 機能を使用して接続しているデバイスに、これらの IP アドレスを割り当てます。Web セキュリティ アプライアンスは、設定されているいずれかの IP アドレスからトランザクションを受信すると、そのユーザをリモート ユーザと見なします。この設定では、Web セキュリティ アプライアンスが適応型セキュリティ アプライアンスと通信しません。
- **Cisco ASA との統合**：Web セキュリティ アプライアンス管理者は、1 つ以上の適応型セキュリティ アプライアンスと通信するよう Web セキュリティ アプリケーションを設定します。適応型セキュリティ アプライアンスは、IP アドレスとユーザのマッピングを保持し、その情報を Web セキュリティ アプライアンスに伝達します。Web プロキシはトランザクションを受信すると、IP アドレスを取得して IP アドレスとユーザのマッピングをチェックし、ユーザ名を特定します。適応型セキュリティ アプライアンスと統合すると、リモート ユーザのシングル サインオンを有効にできます。この設定により、Web セキュリティ アプライアンスは適応型セキュリティ アプライアンスと通信します。

- [追加（Add）] : 適応型セキュリティ アプライアンスが通信できる Web セキュリティ アプライアンスを 1 つ以上追加できる [アクセス コントロール設定の追加（Add Access Control Configuration）] ダイアログボックスを開きます。
- [編集（Edit）] : 選択した接続の [アクセス コントロール設定の編集（Edit Access Control Configuration）] ダイアログボックスが開きます。
- [削除（Delete）] : 選択した接続をテーブルから削除します。確認されず、やり直しもできません。

ステップ 2　モバイル ユーザ セキュリティ サービスをイネーブルにする場合、VPN を介してクライアントと接続を開始します。Web セキュリティ アプライアンスは、適応型セキュリティ アプライアンスと統合するように設定されると、初回起動時に、設定されているすべての適応型セキュリティ アプライアンスと HTTPS 接続を確立しようとします。接続が確立されると Web セキュリティ アプライアンスは、設定されている ASA アクセス パスワードを使用して適応型セキュリティ アプライアンスを認証します。認証が正常に行われると、適応型セキュリティ アプライアンスは Web セキュリティ アプライアンスに IP アドレスとユーザのマッピングを送信します。WSA が存在しない場合、ステータスは disabled になります。

ステップ 3　サービスをイネーブルにする場合、サービスのどのポート番号を使用するかを指定します。ポートの範囲は 1 ～ 65535 で、管理システムにより WSA にプロビジョニングされた対応する値と一致させる必要があります。デフォルトは 11999 です。

ステップ 4　必要な場合、WSA アクセス パスワードを変更します。適応型セキュリティ アプライアンスと Web セキュリティ アプライアンス間の認証に必要な Web セキュリティ アプライアンス アクセス パスワードを変更できます。このパスワードは、Web セキュリティ アプライアンスに設定されている当該パスワードと一致する必要があります。

ステップ 5　[WSA アクセス パスワード（WSA Access Password）] フィールドで、ASA と WSA 間の認証に必要な共有秘密パスワードを指定します。

ステップ 6　指定されたパスワードを再入力します。

ステップ 7　[WSA セッションの表示（Show WSA Sessions）] により ASA に接続された WSA のセッション情報を表示できます。接続されている（または接続された）WSA のホスト IP アドレスおよび接続時間がダイアログボックスに返されます。

エンドポイントから WSA にトラフィックをリダイレクトするプロキシ サーバの設定

エンドポイントからの Web トラフィックを WSA にリダイレクトするように、Web プロキシを設定する必要があります。これを行うには、WCCP ルータを使用してトランスペアレント プロキシを設定するか、次の手順を実行して明示的なプロキシを設定します。

ステップ 1　ASA 上で ASDM を起動し、[リモート アクセス VPN（Remote Access VPN）] > [ネットワーク（クライアント）アクセス（Network (Client) Access）] > [グループ ポリシー（Group Policies）] を選択します。

ステップ 2　Web vpn 用に設定されているグループ ポリシーを選択し、[編集（Edit）] をクリックします。

ステップ 3　[内部グループ ポリシーの編集（Edit Internal Group Policy）] ウィンドウの左ペインで、[詳細（Advanced）] ノードを展開し、[ブラウザ プロキシ（Browser Proxy）] を選択します。

ステップ 4　[プロキシ サーバ ポリシー（Proxy Server Policy）] エリアの [継承（Inherit）] をオフにします。

ステップ 5　[以下からプロキシ サーバの設定を選択する（Select proxy server settings from the following）] を選択し、[下記のプロキシ サーバの設定を使用する（Use proxy server settings given below）] をオンにします。

ステップ 6　[プロキシ サーバの設定（Proxy Server Settings）] エリアを展開し、[サーバ アドレスおよびポート（Server Address and Port）] の [継承（Inherit）] チェックボックスをオンにします。WSA の IP アドレスおよびポート番号を指定します。

ステップ 7　[ローカル アドレスに対してサーバをバイパスする（Bypass server for local addresses）] の [継承（Inherit）] チェックボックスをオフにし、[はい（Yes）] を選択します。

ステップ 8　プロキシ サーバ経由でアクセスしないアドレスのリストを入力する場合は、[除外リスト（Exception list）] の [継承（Inherit）] チェックボックスをオフにし、IP アドレスを入力します。[除外リスト（Exception list）] エリアで、これらの IP アドレスを例外に指定できます。

ステップ 9　[OK] をクリックします。

ステップ 10　[適用（Apply）] をクリックします。